JPRS-JST-90-011
26 FEBRUARY 1990

FOREIGN
BROADCAST
INFORMATION
SERVICE

JPRS Report

Science & Technology

Japan

KEY TECH CENTER

ADVANCED COMMUNICATIONS RESEARCH

JPRS-JST-90-011
26 FEBRUARY 1990

SCIENCE & TECHNOLOGY
JAPAN

KEY TECH CENTER ADVANCED COMMUNICATIONS RESEARCH

906C3822 Tokyo KODO SOGO TSUSHIN GIJUTSU CHOSA HOKOKUSHO in Japanese Mar 89 pp 1-109

CONTENTS

Preface.. 1

Advanced Communications Technology Research Committee............... 2

Table of Contents.. 3

Chapter 1. Introduction.. 4

Chapter 2. Trends of Advanced Communications Technology Used in Advanced Communications Networks........................ 14

Chapter 3. Advanced Communication Network Technology.............. 29

Chapter 4. Measures for Utilization of AI Technology in Advanced Communication Networks.................................. 56

Chapter 5. Security Technology in Advanced Communications Networks. 65

Supplement.. 76

Chapter 6. Conclusion.. 85

Key Tech Center Advanced Communications Research

906C3822 Tokyo KODO SOGO TSUSHIN GIJUTSU CHOSA HOKOKUSHO in Japanese Mar 89 pp 1-109

[Report by the Japan Key Technology Center]

[Text] **Preface**

Advanced communication technologies are fundamental for an advanced information society. Today, information telecommunication systems are being networked through interconnections, and it is expected that such systems will play a leading role in the future flow of advanced information. Therefore, in order to predict future technological developments, it is necessary to elucidate the themes of the development of communication technologies related both to network construction and administration, and to analyze user needs sufficiently.

From this perspective, the Key Technology Center initiated its "Research in Advanced Communications Technology" project. Designed as a 3-year project, it was launched in FY 1986. In FY 1986, we analyzed user needs in terms of the jobs to be processed by networks and the requisite job processing level, thereby elucidating the environment for the development of advanced communications technology. In FY 1987, we studied the trends of the development of advanced communications technology by systematically examining network interconnection technology, network resource management technology, network administration and management technology, etc., and identified urgent technical themes. Finally, in FY 1988, we examined the trends of advanced communications technology in terms of advanced communications networks. We also assessed the possibility of utilizing artificial intelligence (AI) technology, explored security technology, and identified themes applicable to advanced communications networks.

The final stage of research is summarized in this report, which deals with FY 1988. We would be very happy if this report can be used as basic material in this field for promoting tests and research into key technologies and for helping in the establishment of related measures. We express our deep gratitude to the Telegraph and Telephone Technology Committee, which was entrusted with the research and made great efforts to carry it out. We are also grateful to various research groups and individuals in the Ministry of Posts and Telecommunications for their guidance and cooperation. March 1989. Key Technology Center.

Advanced Communications Technology Research Committee

Chairman:

Shoichiro Asano	Professor, Science Information Center

Members:

Yuji Arai	Subsuperintendent, Totsuka Factory, Hitachi, Co.
Osamu Hashimoto	Deputy manager, Switching Planning Office, NEC Corp.
Kinji Ono	Manager, Kami-Fukuoka Laboratory, KDD Corp.
Hisamitsu Motome	Manager, Networking Promotion Office, Data Communications Division, Telecommunications Department, Telecommunications Bureau, Ministry of Posts and Telecommunications
Toshiaki Shibayama	Adviser, Daiichi Kangyo Bank
Noboru Takayanagi	Chief engineer, Intec
Kenji Naemura	Center, NTT Corp.

Observer:

Key Technology Center

Secretariat:

Ken Hasegawa	Manager, Planning Department, TTC
Toshimichi Tsukaya	Manager, Third Engineering Department, TTC

Table of Contents

Preface

Chapter 1. Introduction

1.1 Development of Information Communications in Japan (Summary)
1.2 Problems in Intersystem Connection
1.3 Targets of Research Into Advanced Communications Technology

Supplement Summary of Research in FY 1986 and FY 1987

Chapter 2. Trends of Advanced Communications Technology Used in Advanced Communications Networks

2.1 General
2.2 Trends in Standardization Related to Advanced Communications
2.3 Systematic Arrangement of Technical Themes Around User Networks

Chapter 3. Advanced Communications Network Technology

3.1 User-Defined Network Technology
3.2 Network Structure Concealment Technology
3.3 Telecommunications Management Network

Chapter 4. Measures for Utilization of AI Technology in Advanced Communications Networks

4.1 Present Status of AI Technology: Its Application in Communications Networks
4.2 AI Support Technology Used in Network Design
4.3 AI Support Technology Used in Network Management and Administration
4.4 AI Support Technology Used in Network Maintenance
4.5 Future Themes

Chapter 5. Security Technology in Advanced Communication Networks

5.1 Trends of Standardization
5.2 Present Status of Security Technology
5.3 Future Themes

Chapter 6. Conclusion

Chapter 1. Introduction

1.1 Development of Information Communications in Japan (Summary)

In the approximately 25 years that have elapsed since they were first conceived, advanced communications networks in Japan have been incorporated into economic and social activities, and are continuing to expand dramatically. From the functional perspective, conventional means of communications such as the telephone and telegraph can be regarded as extensions of the functions of the human mouth, ears, hands and eyes, because they transmit and exchange spoken voice messages or letters as they are. But advanced communications are revolutionary in that they employ the functions of the human brain, such as thought and memory, in the world of communications.

In other words, communications originally designed to be used simply as aids to human activities can now substitute for many human activities, and in some instances can even function as independent economic and social activities.

Consequently, the utilization of advanced communications networks does not consist of working out how they are to be used by taking their functions as preconditions, but it is now possible to consider them from an enterprise-oriented perspective, for example, how business activities are to be combined in a communications network.

The development of advanced communications networks in Japan can be summarized as follows.

(1) In the decade from 1965 to 1975, individual companies started to construct in-house systems of focused data communications, and such networks became established. These networks were most often limited to individual companies, so this decade may be regarded as the period of development of "zero-dimensional" information communications.

(2) In the next decade, from 1975 to 1985, individually constructed in-house systems began to be connected to one another. This trend is understandable because no business activities are restricted to within one company but they are based on a variety of exchanges between companies. But it is also true that connections between companies vary greatly in different fields of industry. International connections in the same industry have been implemented in the banking and airline industries. But in other fields it was often after 1980 that primitive forms of connections, such as the private connection between two systems via tie lines or connections between the center of one company and the terminals of another company via the public telephone network, started. Although the necessity of communications from an economic viewpoint began to be recognized, this decade can be regarded as the period of "one-dimensional" information communications when the general expansion of networks was considered.

(3) The current decade began in 1985. The telecommunications business was liberalized in April 1985. For those constructing systems, this meant a lower tariff thanks to the introduction of competition, more options in the

selection of the network services to be used, and, from a different perspective, opportunities to construct and provide a network with the services they need themselves. One type of network that attracted considerable attention at that time was the value-added network (VAN). The enthusiastic expectations surrounding VANs were based on the need to solve such problems as the complex circuit installation process, waste, and nonmatching protocols that could interfere with intersystem connections.

As of 1 February 1989, more than 650 companies were registered as VAN carriers (Type II telecommunications carriers). However, many were far from the firm establishment of business foundations due to the necessity of preliminary investments prior to entering the communications business, lack of talent, etc. Further, the added values of their services must continue to advance in the future.

Nevertheless, this decade is a promising period in which information communications are expected to expand further. Intersystem connections have also transcended the barriers of individual industries, leading to interindustry communications. Thus this decade is worthy of being called the period of "two-dimensional" information communication. Now that the information being disseminated contains not only data but also integrates voices and images, we can say that the advanced communications networks in the real meaning of the term appeared in this decade.

1.2 Problems in Intersystem Connection

Above, we have described the process of the development of data communications systems in Japan. Since communication systems are being constructed according to enterprise-oriented thinking, as previously noted, the matching of system technology and business activities has become indispensable. And even when matching has been obtained, periodic reexamination is always necessary because both of these factors are variable.

Larger intersystem connections have been limited primarily to instances where the following conditions apply:

(1) First, where there is participation in a large system of international business interconnection such as SITA and SWIFT.

(2) Similar to case (1) above, but where the necessity for the business is very urgent, such as the Zengin system.

(3) Where one company has a larger voice that makes it capable of promoting and obtaining permission to connect from the companies concerned.

(4) Where such an interconnection is required to increase bargaining power in business or local activities.

It must be noted, however, that these conditions are largely dependent on the specific circumstances of an individual company or on the present status of an industry, etc. Thus there should naturally be a limit to leaving the initiative for connection to the industry.

Also, from the viewpoint of overcoming factors in business that could interfere with implementation, there must be an approach supporting the technical aspects of interconnection. In this context, it is very important to grasp the limitations of present technologies and, with this in view, to try to determine what technical developments will occur in the future.

1.3 Targets of Research Into Advanced Communications Technology

This research is an attempt to identify current technical themes and to establish the direction of development. The research period covered 3 years, from FY 1986 to FY 1988.

The research findings for the first 2 years are summarized in the Supplement following this section. In addition, a short outline of the transition between each of the 3 years is described below.

In FY 1986, questionnaires were sent out to acquire the data that would be used in the basis of our examination. Our goal was to determine the present status of systematization in user companies and to identify their needs for the future.

In FY 1987, we identified the technologies required for interconnection and systematically examined trends.

However, the technologies are continuing to progress. After the construction and initial operation of the ISDN network, which is replacing the current telephone network and which is regarded as the key telecommunications network as we approach the 21st century, several new technologies capable of renovating current telecommunications networks and improving their operability have been announced. These include the VPN (virtual private network), which has led to radical innovations of network configuration, and AI technology, which is expected to make networks more intelligent.

FY 1988 was the year in which the direction and themes for advanced telecommunications in the near future were examined based on current technical progress.

We believe that the continuing development of information communications represents one of the most significant trends of modern society, and that the bases for two-dimensional information communications as described above will also continue to grow and become more sophisticated. We would be very happy if this report can serve as a stimulus for their development.

Supplement Summary of Research in FY 1986 and 1987

1. Targets of Research

Networking centered around data communications is underway based on progress in information communications technology and the growth and diversification of user needs. In particular, networking in industrial fields is developing from individual networks designed for the integration of business operations within a single company to transverse networks connecting several companies. Not only within individual networks but also between several networks, it has become very desirable to enlarge the number of jobs processed across the entire spectrum from production control to shipping information, order receipt/issue and settlement. It is also necessary to improve the level of job processing by such means as the consolidated processing of different jobs, etc.

To achieve these targets, it is essential to improve individual network functions and to develop internetwork connection technology to create foundations capable of supporting the future industrial society.

The previous development system was under the leadership of vendors, with individual vendors developing technologies for both the system construction and administrative aspects--for example, network function expansion and internetwork connection technologies--and provided them to users. However, as user needs are becoming more advanced and increasingly diversified, development leadership is shifting to the users themselves, as reflected by the construction of networks by users using equipment from different vendors and by the improvement of overall network administration efficiency by means of connections to other networks required for the users' own networks.

Therefore, technical developments in the future should stress the development of interconnection technology from the aspects both of network construction and administration by incorporating user needs.

Our research was conducted over a 3-year period in order to identify the themes for such technical developments.

2. Outline of Research in FY 1986

2.1 Targets and Methodology of Research

The research in FY 1986 consisted of sending a questionnaire to a sample of 300 companies selected from the companies listed in the First and Second Sections of the Tokyo Stock Exchange, insurance companies and other major companies. We were careful to avoid overemphasis on specific industries. The purpose of the questionnaire was to determine user needs in terms of the jobs processed by the network and the job processing level, and to define the environment required for the development of advanced communications technology in the future. The principal categories are listed below:

(1) Types of jobs being performed at each user company.

(2) Among the jobs in (1), the types of jobs for which data communications are performed.

(3) Types of jobs to which the user company hopes to apply data communications.

(4) Status of connection and problems, etc.

The questionnaire results were analyzed and examined by the members of the committee.

2.2 Results of Research

The research in FY 1986 was an approach from the user side to clarify the technical environment needed for the development of advanced communications technology. The results of the research concerning the jobs handled by the users on networks, network functions used at that time, themes concerning interconnection between networks, etc., are as follows:

(1) The jobs being handled by current data communications consisted mainly of order receipt/issue and goods transactions, sales inventory control and accounting, and financial control.

(2) The jobs expected to be handled by future data communications consisted mainly of management information control, accounting and financial control, and order receipt/issue and goods transactions. With respect to other jobs, those which had not often been networked before were expected to be networked relatively more than other jobs.

(3) The functions currently being implemented through the network were examined in terms of both jobs and companies, but it was found that the general trends were the same. The level of functions that were being implemented was higher in larger-scale companies.

(4) The functions expected to be implemented through the network in the future were bidirectional transmission and synchronous transmission in terms of jobs, and the functions that are expected to have a particularly high implementation rate compared to the current rate were medium conversion and 16 and 64 kilobit/s operations. From the perspective of companies, the functions expected to be implemented were bidirectional transmission and 9.6 kilobit/s operation, while those expected to show a higher implementation rate than the current rate were media conversion and signaling system conversion.

(5) Of the companies surveyed, 69.9 percent had already established connections between networks or were planning to do so. From the viewpoint of business fields, the interconnection rate is high in the service, commercial and manufacturing industries.

(6) Points of dissatisfaction or points requiring improvement in the current or planned system interconnections were in the following order:

—The impossibility of protocol matching with connection destination.

—The difficulty in determining the division of responsibilities.

—The impossibility of distinguishing between failures in the remote system of the other party and the local system.

(7) Consequently, the major themes for interconnections are as follows:

—The standardization, unification and rational conversion of communication systems.

—The unification of administrative rules, etc., applied to connections.

—The standardization of connection points, such as the division of responsibilities.

—Measures to reduce faults and increase reliability.

(8) In addition, a free-answer question was asked about the solutions necessary for network interconnection problems and problems to be solved. The answers were in the following order:

—Unification and standardization of communication protocols.
—Enhancement of network administration and management.
—Assurance and enhancement of security.
—Clarification of administrative rules.
—Countermeasures against the failures of communication lines, etc.

These five problems can be regarded as user requirements for interconnections between networks.

2.3 Future Themes

As a countermeasure against network interconnection problems in the future, it will be necessary to make further advances in administration and management technology. With regard to network management functions in particular, uniform and single-vendor type management technologies provided by system manufacturers as carriers are available, but a general-purpose network management technology of the multivendor type has not been achieved yet. Considering the development of diversified and advanced business links, the development of such technologies should be positioned as an important item for networking in the future.

Considering the application of digital technology and ISDN to public networks as well as the appearance of diverse carriers and different media from previous technologies such as satellites, it will be necessary to achieve physical matching in connections.

The promotion of advanced communications necessitates various technical developments. In our research in FY 1986 to determine the environment for the development of advanced communications technology in the future, it became clear that three technologies—development of network interconnection technology, network resource management technology and network administration technology—are most important for supporting advanced communications.

3. Outline of Research in FY 1987

3.1 Targets and Methodology of Research

Based on the research of the previous year, the research in FY 1987 systematically examined detailed elements of technology to elucidate the trend of development of advanced communications technology.

3.2 Research Items

Based on the results of our research in FY 1986, the element technologies required for the implementation of advanced communications technology were classified into the following three categories, and each of them was examined in detail:

(1) Network interconnection technology

This is technology for connecting individual networks organically and efficiently. It is technology that can be positioned as a fundamental technology for the promotion of advanced communications.

—Protocol standardization, unification and conversion technologies.

—Unification of administration rules applied to connections.

—Technology to avoid increasing response time which occurs as a result of interconnection.

—Standardization of connection points, such as the division of responsibility.

(2) Network administration technology

This is technology concerning the concrete management capabilities of individual networks that should be the condition for developing network interconnections.

—Technology for maintaining a high degree of safety and reliability for network interconnection and network resource management.

—Technology for facilitating network modification, etc.

(3) Network resource management technology

With the diversification of the uses of information communications and the increased possibilities of communications,1 this technology provides an integrated function to identify the target of communications and to acquire the techniques and information necessary to achieve communications. It can be positioned as the foundation of future advanced communications.

—Technology for supporting directory and access control, which enables users to understand the locations of network resources (various information communication resources on the network, such as data bases, host computers and terminals), access them with simple procedures, and combine and utilize them properly.

—Technology for assuring security.

3.3 Network Interconnection Technology

Each network oriented toward information processing is a multivendor type of network individual to each user. Since the information it handles is not derived from a flexible human being but from information source such as computers and various kinds of data equipment, the conditions for interconnection are diversified in several layers and each of them needs to be carefully defined.

As ISDN will be available in addition to existing networks, it was pointed out that the provision of technology for smoothly maintaining mutual communications between networks is an important theme associated with the interconnection of networks. In an age when there were only a few types of networks and the relationships between them were rather simple, interconnection between different types of networks was not regarded to be important. But the problem of interconnection between different types of networks has become unavoidable as a result of the appearance of networks related to both voice and data, such as ISDN.

Of the communication functions at a higher level than the basic network, protocol and media conversion technologies are the most important. It is important to seek to ensure their proper implementation and standardization.

In addition, it was also pointed out that the conformance test, which checks information communication equipment against international standards, is gaining an important position as a foundation for maintaining communications ability.

3.4 Network Administration Technology

Following the diversification, advances and widespread expansion of network system services, the influence and role of communications systems in the information society has become greater and the importance to network administration technology has increased. With respect to these phenomena, we arranged the functions, element technologies, themes, etc., of nonstop technology, virtual networking technology and billing technology, which are required for reliability and services on the user system side, and of the human interface technology and knowledge processing technology that are required for the operation, management and support on the network administration side. As a result, we were able to clarify the conditions necessary for the systematization and unification of administration.

The current services provided by the networks are based on physical network operations determined by the connections of hardware, such as switches, in a fixed way. Therefore, the services provided by the network are restricted by the limitations of hardware operations.

On the other hand, it was pointed out that progress of network administration organizations utilizing software techniques—for example the implementation of several virtual networks by configuring logical groups of network users within a single physical network or the increase of network flexibility by means of dynamic traffic control—represent an important technical theme for meeting the requirements of the advancement and diversification of services.

3.5 Network Resource Management Technology

Following advances in information communications, the importance of network resource management technology has become recognized. It is a product of the diversification of information communications utilization, progress in interconnections between communication networks, the increased necessity of the right to information and privacy, and the recognition of system safety as a social problem.

The first problem pointed out related to network resources was their diversification. That is to say, not only the communications equipment, but also the computers, data bases and job processing software have to be recognized collectively as communications resources. It is the network resource management services that effect smooth communications between resources, while network resource management technology is the technology to achieve this.

On this occasion in particular, the importance of a directory system as a means for improving the freedom and convenience of information communications was made clear, and the necessity of developing concrete measures for the implementation and administration of directories has been pointed out as one way to make this possible.

Meanwhile, to maintain the safety of communications between resource, it is important to prevent artificial disturbance of the networks. The problems of network resource access control support and the related security technology also arise in this connection.

3.6 Urgent Technical Themes

Among the problems cited above, the following were cited as technical development themes with greater urgency.

For present themes of technical development, it was pointed out that protocol conversion technology in the higher layers for combining various applications in electronic mail and personal computer communications, which are showing rapid growth, would be one of the most important themes in the future.

The most important theme with respect to network administration turned out to be a general examination of the improvement of the reliability of hardware as well as administration software.

As one of the subjects of network resource management, it would be necessary to advance the concrete support functions for users of directory systems.

In addition to the above, it was also pointed out that it is critical to establish AI technology for the construction and effective use of more advanced and complicated information communications networks. It is also necessary to establish distributed processing technology for efficient distribution and organic coupling through the communications channels of processors, which are the basic elements of nodes, and information resources in various locations in the network, as commonly fundamental technologies for advanced communications.

Chapter 2. Trends of Advanced Communications Technology Used in Advanced Communications Networks

2.1 General

To communicate information, it is necessary to maintain the matching, both physical and logical, of the conditions for smooth interconnections between the equipment comprising the systems. The conditions for interconnections are called the standards.

Standards are created at various levels, such as international standards, local standards, national standards, group standards and company (in-house) standards.

In the world of communications, interconnections are the original, basic condition. In other words, the fundamental purpose of communications is to be able to transmit information to anyone, anywhere. For this purpose, there are the CCITT (International Telegraph and Telephone Consultative Committee, which deals with technology and administration related to telecommunications networks) and the CCIR (International Radio Consultative Committee, which deals with technology and administration related to radio communication networks). The CCITT, in particular, plays a leading role in the standardization of various matters required for interconnections in telecommunications. The CCITT announces recommendations for the technological and administration aspects of telecommunication systems, which are decided by the unanimous vote of the assembly. For example, ISDN is also defined by one of the recommendations of the CCITT, and is a communication system implemented based on the "integrated services digital network" recommendations represented by reference symbol "I."

The ISO (International Standardization Organization) conducts standardization activities related to computers. The ISO now maintains close contact with the IEC, and they have established a joint technical committee named the ISO/IEC JTC1.

OSI (open system interconnection) is network architecture promoted under collaboration between the CCITT and JTC1.

Standardization in the world of information is conducted by CCITT and JTC1, which contact each other to avoid problems in case of fundamental subjects used as an international standard, such as OSI.

Local standards are often created for political reasons or due to the specific requirements of a particular area. For example, in eastern Europe, the standards are different from the European standards (EN) and use a different encoding compression ratio due to the length of circuits in the initial stage of PCM communications in North America (both u-LOW of North America and A-LOW of Europe are standardized now). However, when an information network on a global scale is completed, theses standards are expected to be absorbed into the international standard.

In addition to these standards, the authorities of each individual country also create their own national standards for domestic use. These standards are promoted by granting permission for the use of approved products marked as conforming to the standards. In principle, national standards should be incompliance with international standards. However, due to the specific problems of each country, such as language problems, it is, in general, unavoidable that some provisions supplementing international standards have to be defined.

Moreover, there are group standards that are standardized and proposed by approved private standardization organizations. Examples of such organizations include the TTC in Japan and, though the field covered is different, UL standards, which are safety standards adopted by the insurance industry in the United States. Similar to the cases cited in these examples, standardization of some new fields in which rapid progress is taking place is done under the leadership of certain academic societies.

2.? Trend of Standardization Related to Advanced Communications

For the research term from 1989 to 1992, the CCITT is planning to undertake the following standardization activities for advanced communications: research into the data communications at SGVII, research into terminal equipment for telematic services at SGVIII, research into telecommunication languages and techniques at SGX, research into ISDN at SGXVIII, etc. These research projects cover themes related to the promotion of ISDN, while the research into telecommunication network management (TMN) at SGIV is worthy of attention because of its relevance.

The OSI standard, or "open system interconnection" standard, is intended to enable free information exchanges through interconnections of computer terminal equipment with different functions. OSI is being standardized through collaboration between CCITT and JTC1. This work has been underway since 1977.

Communications through advanced communication systems are not possible unless the information exchange methods, formats and sequences of the equipment composing the network are defined. Here the importance of computer network architectures arises, for it systematically defines the rules (protocols) enabling logical expressions of the components such as the computers, networks and terminal equipment, their interconnections, and communications between them. At present, different computer network architectures have been developed and are proprietary to individual manufacturers. To make communications between different computer models possible, those architectures should be internationally standardized. This can be achieved by standardizing the protocols until the point is reached where each computer can be connected at the user program level (application layer) to provide compatibility with various network configurations including private lines and telephone lines as well as data networks (circuit switched, packet switched) and LAN and ISDN. This will also permit the configuration of systems that can communicate equally with any computers, from personal computers to mainframes. It is expected, therefore, that advanced man-machine interfacing—

including multimedium interface (codes figures, etc.) and the coexistence of diverse, advanced job processing operations such as electronic mail file management and multimedia switching--will be made possible.

Table 2.2.1 lists the major international standardization organizations related to advanced communications.

Table 2.2.1 Major International Standardization Organizations Related to Advanced Communications
(Source: Denshi Joho Tsushin Handbook)

Standardization organization		Outline of standardization contents
CCITT	SGVII	OSI reference models, common protocol for LSI layers and message handling system (MHS) protocols, from the viewpoint of data network configuration and application.
	SGVIII	Terminal equipment and protocols for telematic services (generic term for telex, facsimile, videotex, etc.)
	SGX	Protocol format description techniques, etc.
	SGXVIII	User-network interface of ISDN (corresponds to protocols from the physical layer to the network layer).
ISO/IEC	JTC1/SC 6	Protocols of OSI lower layers (physical layer to protocol layer). LAN-related protocols (mainly related to the physical layer and data link layer).
	JTC1/SC18	Document communication protocols (related to the application layer and presentation layer).
	JTC1/SC20	Data encryption protocol (related to the data link layer, transport layer, presentation layer, etc.)
	JTC1/SC21	OSI basic reference model. Protocols for OSI higher layers (session layer to application layer). Protocol format description technique, conformance testing technique. Command response languages for data bases and operating systems.
	JTC1/SC24	Computer graphics.
	MTC1/SG-FS	Function standards.

OSI includes the use of basic logical and virtual concepts. The logically defined basic components consist of the "application process," which is the subject of intersystem communications,; the "open system," which executes processing, etc., according to OSI rules; the "physical media," which include interconnected communication circuits; and the "connection," which refers to the logical communication channel that is not conscious of the media. System component resources such as files and data bases are all considered "virtual." Interconnections between models are performed via virtual files, data bases, documents, terminals, etc., whose attributes and configurations are standardized from the viewpoint of the application process so that the number of combinations of conversions is reduced.

7. Application layer

   Controls data processing between user processes

6. Presentation layer

   Controls data expression format between user processes

5. Session layer

   Controls conversation between user processes

4. Transport layer

   Controls data transfer between end systems

3. Network layer

   Controls relay of data transfer path

2. Data link layer

   Controls data transfer between adjacent systems

1. Physical layer

   Controls communication circuits

Figure 2.2.1. Functions of Layers

OSI consists of a total of seven layers. The three lower layers—"physical," "data link" and "network"—deal with the implementation of a transparent, highly reliable data circuit between equipment. The four higher layers—"transport," "session," "presentation" and "application"—function to enable actual communications between the application processes on the equipment by using a data circuit created by the lower layers. Each of the layers has an internally closed protocol standard as its basic standard.

In this way, OSI provides excellent compatibility, ensures standards without the payment of royalties and free equipment procurement from multiple vendors, and facilitates rapid internationalization of business activities. These advantages are attracting attention in many companies, where efforts to put OSI to practical use are underway.

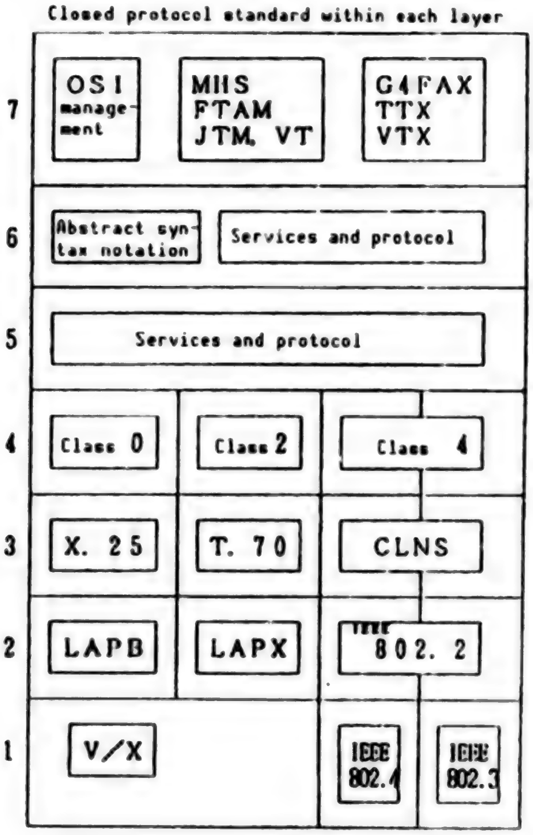


Figure 2.2.2. Basic Standard

With INS Net 64 available since 1988 and the subsequent extension of its service features (D channel packet, etc.), and with the provision of wider service features by INS Net 1500 in 1989, ISDN services in Japan have just entered the period of diffusion. ISDN services are also available in the United States, although they are still in the experimental stage.

ISDN has effected communications, especially conventional communications networks centered around telephones, in a number of ways. The first was the extension of control lines to subscribers. Although conventional telephones provide separate, logical control lines between switching offices, such as the common channel signal links, subscriber terminals are telephone sets with a century-old history. Their control performance can be regarded essentially as just low-speed data lines coexisting with communication lines, though this may be enlarged by the use of touch-tone dialing. In addition, telephones use communications within the voice frequency band, and all communication contents must conform to the analog information line format. In contrast, ISDN provides high-quality 64 kilobit/s, 16 kilobit/s and even 1.5 megabit/s digital lines. As a result, the transmitted signal does not have to be a voice signal at all, provided that it can be a flow of digital codes. This offers new and expanded possibilities for telecommunications.

Further, exchanges of signals including control signals can be performed in a complicated multifunction manner, making it possible to provide new service features.

As manufacturers other than those in the telephone and facsimile fields are expected to participate in the manufacturing of terminal equipment in the future, a test organization may be required to check ISDN interconnections with respect to a wide range of equipment. The area where ISDN connection is possible is still limited at present. It is expected that ISDN will be arranged as early as possible to help promote the diffusion of ISDN terminals.

Figure 2.2.3 shows the ISDN protocol system recommended by the CCITT in 1988. In the figure, the user network interface handles the communication functions of the users and the No 7 signaling system deals with the functions related to the network control.

From the viewpoint of standardization, it can be said that basic problems have generally been solved and that the system has generally been defined by the recommendations made in 1988. Now the focus of standardization is shifting to wideband ISDN, the preliminary recommendations for which are scheduled to be released soon. For this purpose, the rules have been revised to allow the issue of recommendations even in the middle of a term, without waiting for the opening of the end-of-term Assembly.

Since ISDN is very powerful when used as a network, information entirely different in form from conventional concepts could flow in the network. The kinds of communications ISDN is expected to handle include communications between different models and communications involving conversion between different media, for example between image and facsimile or between data and image. It is anticipated that the advent of ISDN will lift communications to a more advanced stage.

The discussion to this point has focused on international agreements. In Japan, standardization in the area of communications is developed by the TTC, which is a private standardization organization established in October 1985 to create standards related to the connection of telecommunications networks. It organizes standardization conferences to develop criteria for the standardization of interconnections between ISDN and existing networks and between the equipment used in them. The TTC also deals with the standardization of interconnections between PBXs, LANs and VANs.

The basic connection parameters of ISDN have been standardized, but many standards, including the network control standard, have been left for the future.

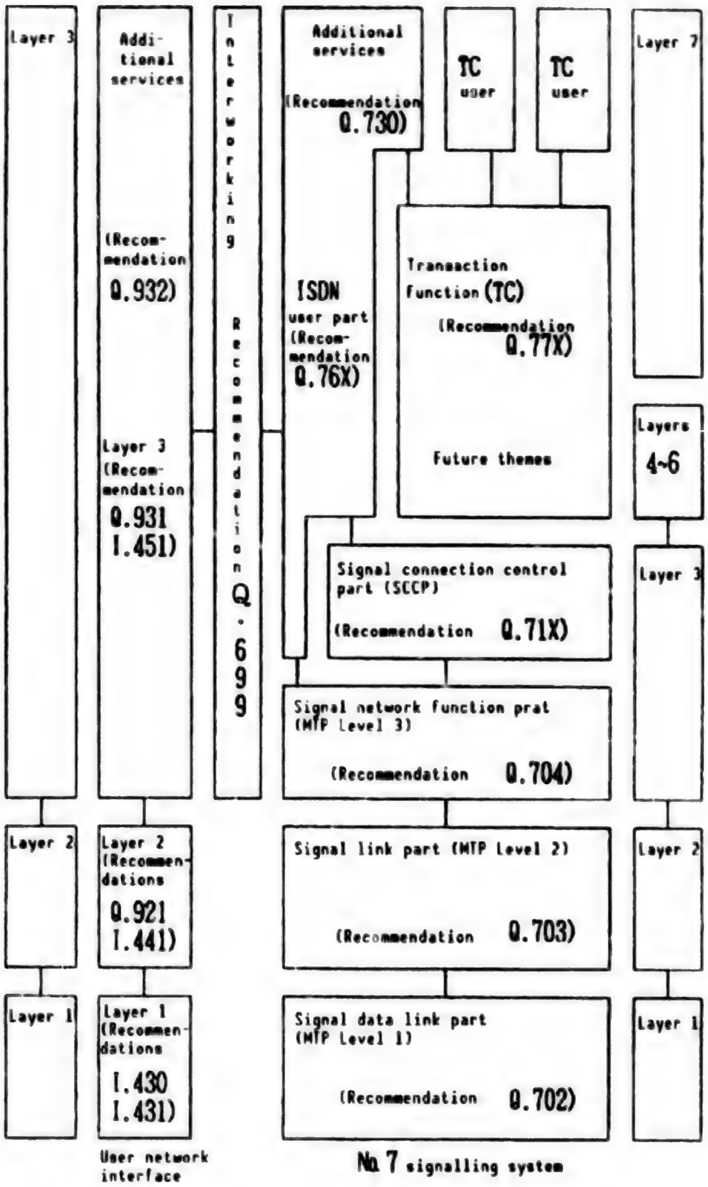

Layer 3
Layer 2
Layer 1
Additional services
(Recommendation Q.932)
Layer 3 (Recommendation Q.931 I.451)
Layer 2 (Recommendations Q.921 I.441)
Layer 1 (Recommendations I.430 I.431)
User network interface
Interworking Recommendation Q.699
Additional services (Recommendation Q.730)
ISDN user part (Recommendation Q.76X)
TC user
TC user
Transaction Function (TC) (Recommendation Q.77X)
Future themes
Signal connection control part (SCCP) (Recommendation Q.71X)
Signal network function prat (MTP Level 3) (Recommendation Q.704)
Signal link part (MTP Level 2) (Recommendation Q.703)
Signal data link part (MTP Level 1) (Recommendation Q.702)
No.7 signalling system
Layer 7
Layers 4~6
Layer 3
Layer 2
Layer 1

Figure 2.2.3. System of ISDN Protocol Recommendations (CCITT recommendations in 1988) (Source: SHISETSU, Vol 40.8)

The number of items that should comply with international standards is increasing year by year. In addition, for items without a corresponding international standard, such as still images, a domestic standard must be created in the meantime. It is also becoming necessary to undertake activities to prevent differences from international standards. In other words, with the rapid progress of communications technology, it may be necessary for us to create a preliminary, domestic standard for something without always waiting for international standardization. At the same time, we should contribute to the creation of an international standard using that preliminary domestic standard.

References

1. Izumi, T., "ISDN Protocol: Trend of Standardization and Themes for Future," SHISETSU, Vol 40 No 8.

2. Ishikawa, H., "Trends of ISDN Services in Foreign Countries," Ibid., Vol 40 No 5.

3. Murata, T., "Start of 'INS Net' Services Exploring the Information of the Highways of Tomorrow," Ibid., Vol 40 No 5.

4. Wakayama, H. and Noguchi, S., "OSI: Open System Interconnection (I)—Basic Concept of OSI," DENSHI JOUHOU TSUSHIN GAKKAI-SHI, October 1988.

5. Information Planning Office, Information Standards Division, Agency of Industrial Science and Technology, MITI, "Handling of Open System Interconnection (OSI) Functional Standards in Industrial Standards," HYOUJUN-KA JOURNAL, Vol 18, October 1988.

6. Kubota, A., "Latest Trends of OSI Conformance Tests: Summary of Test Methods, Test Systems, Test Procedures and Executing Organs," COMPUTER AND NETWORK LAN, December 1988

7. Iwamatsu, Asakura, Kurahashi, Maruyama and Takasawa, "Protocols Used in Demonstrations of Connection Between Different Models at INE '88," Ibid., December 1988.

8. "Material II by the Standardization Technical Committee—Interim Report on Standardization Activities in FY 1988," DENSHI JOUHOU TSUSHIN HANDBOOK, Electric Information Communications Society of Japan.

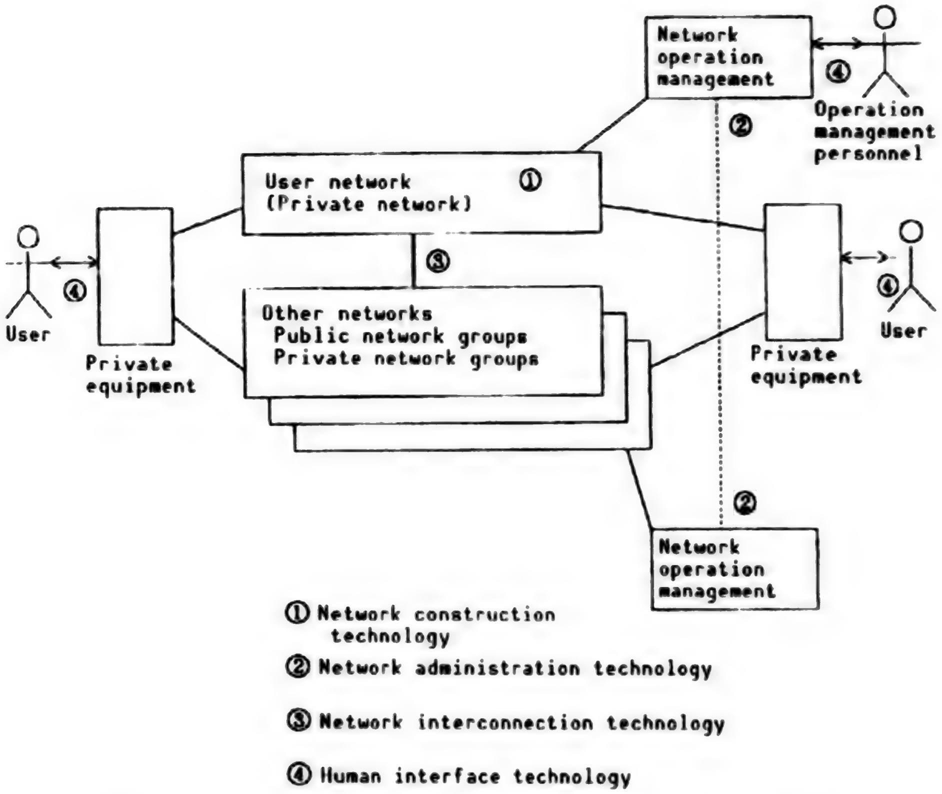
9. "Material III by the Standardization Technical Committee—Middle-Term Prospects for Standardization," Ibid.

2.3 Systematic Arrangement of Technical Themes Around user Networks

In this section, the technical themes of each network element are examined by assuming a model environment surrounding a user network as shown in Figure 2.3.1.

2.3.1 Network Construction Technology

The new telecommunication business law introduced the principle of free competition, and many carriers, network services and communication equipment manufacturers have appeared since it was enacted. In the conditions created by the new law, it is necessary to establish the following types of technologies related to network construction:



Network operation management
④
②
Operation management personnel
User network (Private network)
①
③
④
User
Private equipment
Other networks
Public network groups
Private network groups
Private equipment
④
User
②
Network operation management
① Network construction technology
② Network administration technology
③ Network interconnection technology
④ Human interface technology

Figure 2.3.1. Environment Surrounding User Network

(1) Network design support technology

From the user's point of view, the range of available communications equipment, lines and networks has expanded. At the same time, the complexity and difficulty of selection and user network design have increased. Furthermore, due to the very rapid technical progress and shortened lifespan of individual communications devices, it has also become difficult to estimate the life cycle of a system as a whole.

Such a multivendor environment demands progress in network design support technology. Consequently advanced design support technology and simulation technology, which take the system life cycle into consideration and utilize AI (or knowledge processing) technology, have become important themes.

(2) Technology for increased network reliability

Maintaining the superiority of their information is becoming a matter of life or death for general companies, and faults in networks have a large influence on business activities as well as on general households. This requires the establishment of highly reliable networks, which in turn involves the following technical themes:

a. Technology for increasing the reliability of network facilities

Manufacturing technology related to hardware as well as software.

b. Fault tolerant technology

Technology for redundancy of facilities including equipment and lines.

c. Network security technology

In particular, technology for protection against threats by human elements, such as checking access rights.

(3) Technology for the automatic generation of communications software

It is anticipated that the demand for communications-related software will increase following the advent of networking. However, the development of communications-related software is becoming more difficult for general users because it requires more specialized skills and a different development environment compared to that used for the development of ordinary computer applications. Therefore, support technology is required to make the development and testing of communications-related software easier.

2.3.2 Network Administration Technology

When constructing their networks, users often pay less attention to administration functions. As a result, administration costs (especially personnel expenses) can exceed the equipment cost when the network increases in scale, as shown in Figure 2.3.2. Therefore, technology for saving labor and improving network administration is required.

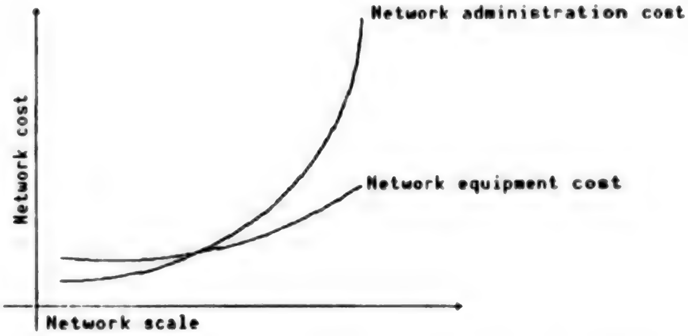


Figure 2.3.2. Network Scale and Costs

(1) Fault management technology

Among the operations required for fault management—which consists of fault detection, trouble shooting and fault recovery—troubleshooting generally occupies the most time. It is particularly dependent on the experience and intuitive ability of the administrative personnel. The following technical measures are required to achieve labor savings.

a. Standardization

More and more network equipment is supplied from multiple vendors, who are increasingly emphasizing functions. However, different vendors provide different administration functions and human interfaces, making integrated management of the whole network difficult. To improve this situation, it is necessary to standardize the interface (management functions and protocols) between the network components and the user's network management functions. The actual implementation of the telecommunications management network (TMN) being examined by CCITT is expected to provide a good solution for this. It is also desirable, however, that the results of standardization be reflected not only among carriers but also among user networks or in the environment of interconnections between user networks. The same thing applies to configuration management, account management, etc., as well as to fault management.

b. AI technology

If the introduction of AI technology into human activities dependent on experience and intuition allows the network and administration system to infer or judge the causes of faults themselves, it will contribute to reducing the burden of fault management that currently rests on users.

(2) Security technology

The concept of security covers a very wide range of issues. It involves several perspectives depending on the specific characteristics of different environments, but here we focus on technology intended to protect networks against human threats. Assuming that it is not possible to provide 100 percent protection against threats, network protection technology can be broken down into the following three technologies:

a. Technology for the prevention of threats

Includes information confidentiality technology, for example, encryption technology.

b. Technology for detection of threats

Includes user authentication technology, access rights management technology and other management technologies.

c. Technology for recovery from threats

The recovery technology for software such as data bases is especially important.

2.3.3 Network Interconnection Technology

It is anticipated that networks that were previously constructed individually for different communications media and services, examples of which are shown in the following table, will be interconnected and developed under the stimulus of progress and the diversification of user needs.

[Table]

Basic communication networks	Advanced communication networks (service networks)
•Subscriber telephone network	•Electronic mail service network
•Packet-switched network	•Personal computer communications network
•Circuit-switched network	•Videotex network
•ISDN	•Facsimile network
•Mobile object communications network	•Various VAN service networks
•LAN	
•MAN	
•Satellite network	

Each user constructs a complete network by combining the user's own network with some of the networks listed above. The following technical themes are important for addressing and increasingly satisfying such needs.

(1) Standardization of interconnection protocols

The protocols for interconnection between the communications networks cited above should be standardized, and efforts in this direction are to be commissioned to international standardization organizations such as the CCITT and ISO, or to domestic standardization organizations.

In addition, the fusion between communications and broadcasting is highlighted as a theme to be examined.

(2) Protocol conversion technology

Even when interconnection at the basic communication level (around OSI Layer 3) is made possible, actual communications will not be available unless the matching of the end-to-end, higher-level protocols is ensured. For example, there is a case in which the interconnection of packet-switched networks could lack flexibility because the inter-PAD protocols corresponding to the existing terminal protocols have not been standardized, even though X.75 has already been ensured.

In this way, protocol conversion technology is required in case standardization cannot satisfy the needs for interconnection or in the process before standardization is achieved. This is especially true in real-time (conversational) communications, where the complement technology for concealing the in-network delay from users will be necessary at the same time as protocol conversion technology.

(3) Medium conversion technology

When networks with different communication object media are cterconnected, medium conversion technology to guarantee end-to-end communications is necessary in conjunction with protocol conversion technology. This technology is expected to be capable of converting media, such as data, voice, still images and moving images, without altering the significance or nuance of their information. This technology is also important from the viewpoint of the human interface technology described later.

(4) Integrated media transmission technology

A basic technology that will enable efficient and integrated communication for all media is expected in the future. The ATM network currently being examined and studied by the CCITT deserves special attention.

(5) Network information management technology

To ensure that networks are interconnectable, it is necessary to develop a technology enabling mutual utilization of discrete elements of network information (names, addresses, etc.) that are managed individually.

Application of the directory system, which is being standardized, is expected for this purpose.

(6) Distributed processing technology

When individual networks are interconnected, the functions or information (data bases, etc.) may be distributed in terms of efficiency and management. Distributed processing is required in such cases; it is also important as a technology for the implementation of a directory system.

2.3.4 Human Interface Technology

Terminals and other kinds of communications equipment are being used in rapidly increasing numbers. Users range from large companies to general households. Therefore, it is expected that user friendly interfaces for general users will be provided by the networks or by the terminals themselves.

As the types of users of communication equipment in general expand, it may also be necessary to classify products according to so-called professional use and for consumer use. Professional-use products are those destined for carriers and large businesses, while consumer-use products are for use by the general public.

The following technical themes can be highlighted from the viewpoint of human interface:

(1) Technology for simplification and improvement of user interfaces

This refers to technology for making private equipment and general communications equipment more user friendly. The factors to be considered are as follows:

a. Operation
b. Input/output system (simplification of use of voice, images, etc.)
c. Unification, standardization of terms, functions and knowledge
d. Design
e. Size reduction

The expected effect of this technology is that, assuming that networks with different user-network interfaces are interconnected to each other, users can perform communications with basically the same operations and interface from anywhere.

(2) Technology for simplification of and progress in human interfaces in administration

As described above, conventional communications equipment and administration systems have been designed for professional use, and general users often find them difficult to use or cannot use all of their functions. This may be due to the fact that specialized knowledge is necessary and that the user interconnection covered only phenomenal events. This difficulty has made it necessary to have a greater number of communications engineers and administrative personnel than would otherwise be the case.

Therefore, also from the viewpoint of administration, it is necessary to improve communications equipment and administration systems by creating an intelligent interface with an inference function for troubleshooting, etc., and by developing technology that is effective in reducing the user load.

(3) Intelligent access technology

This is expected to enable intelligent accesses, a few examples of which are listed below, by utilizing AI technology to introduce the advanced knowledge of human beings. Intelligent network and virtual private network technology in the United States deserve special attention in this respect.

a. Automatic translation communications

Enables translation from one language to another, especially in international interconnections between networks.

b. Fuzzy access

Even when correct information regarding the connection destination is not available, this makes it possible to establish a connection based on the stored fuzzy information.

c. Logical accessing

Makes it possible to effect a connection based on the logical name (individual name) alone, without knowing the physical location of the connection destination.

(4) Advancement of terminal functions

When a user uses several networks as shown in Figure 2.3.3, this can be implemented either through an interconnection between a single-function terminal and network or by access to several networks from a terminal. Both of these forms are expected to coexist in the future, and technology for further improving the functions and integration of terminals is required in this context. It is particularly desirable to implement integration that makes it possible to access several networks simultaneously by means of multiwindow technology.

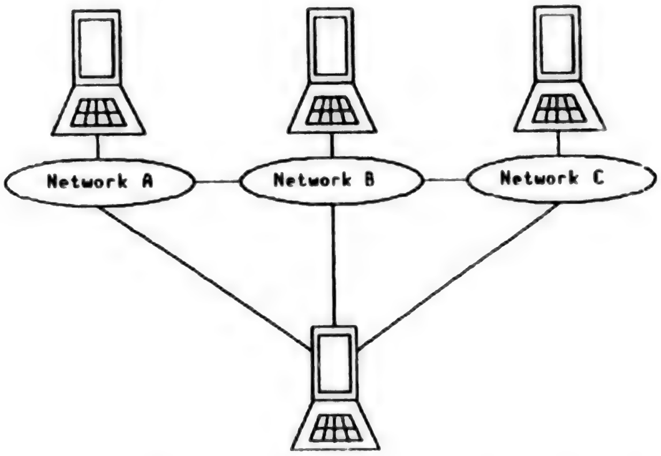


Figure 2.3.3. Example of Network Utilization Form Seen From a Terminal

Chapter 3. Advanced Communication Network Technology

3.1 User-Defined Network Technology

User definition refers to the definition by the user himself of the form and services of the network by changing data in the communications network or by specifying required resources. This allows users to obtain services with tailor-made specifications in place of conventional services based on the specifications defined by the suppliers of the service.

Section 3.1.1 deals with virtual private networks (VPNs). These are user-defined network services that are thought to be the most common from the viewpoint of user needs. They are also the most advanced in terms of practical application.

Next, section 3.1.2 describes service definition technology. This allows users to define service parameters that used to be defined by the carriers and the manufacturers of equipment used in networks.

3.1.1 Virtual Private Network Technology

A virtual private network (VPN) is defined as a service that "physically takes the form of use in common with several users, but that can virtually be regarded as a private network unique to each user." In this section, which deals primarily with the technical aspects of VPN, we will consider the relationship between the scope of VPNs and existing networks; will examine the items to be made unique to each user and the technology involved; and will describe concrete examples of VPNs and the status of standardization.

3.1.1.1 Relationship of VPN construction with existing networks

Existing networks that may have relationships with VPNs include LAN/WANs, urban CATV, private in-house networks, mobile communications and Type II telecommunications businesses (commonly called "VAN"). Figure 3.1.1 shows the relationship between VPN and existing networks.

From the viewpoint of VPN, LAN and WAN are specific physical configurations of private networks. They are, therefore, examined as subsets of private networks.

Since urban CATV has a bidirectional communications function, the method by which it is connected to the public network is examined from the technical aspect. As it is thought that it will function as the equivalent of a public network, its relationship to VPN is a topic to be considered.

From the viewpoint of VPNs, a communications network using mobile transceivers can be regarded as a public network accommodating virtual terminals in each mobile unit, and is therefore handled as a form of hablic network. This fact means that VPN terminals will consist not only of a subscriber's private terminals fixed to subscriber lines, but will also include additional mobile terminals in automobiles, airplanes and ships.

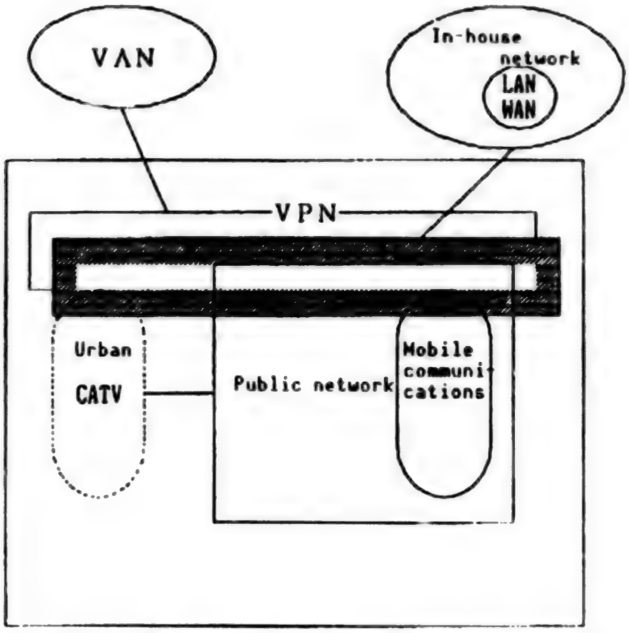


Figure 3.1.1. Relationship Between VPN and Existing Networks

This makes it likely that VPNs centered around mobile units may appear in the transport industry, for example, in the future.

Next, we will examine the relationship between a VPN and the existing networks that utilize it. Figure 3.1.2 shows the relationship between the terminal functions and networks.

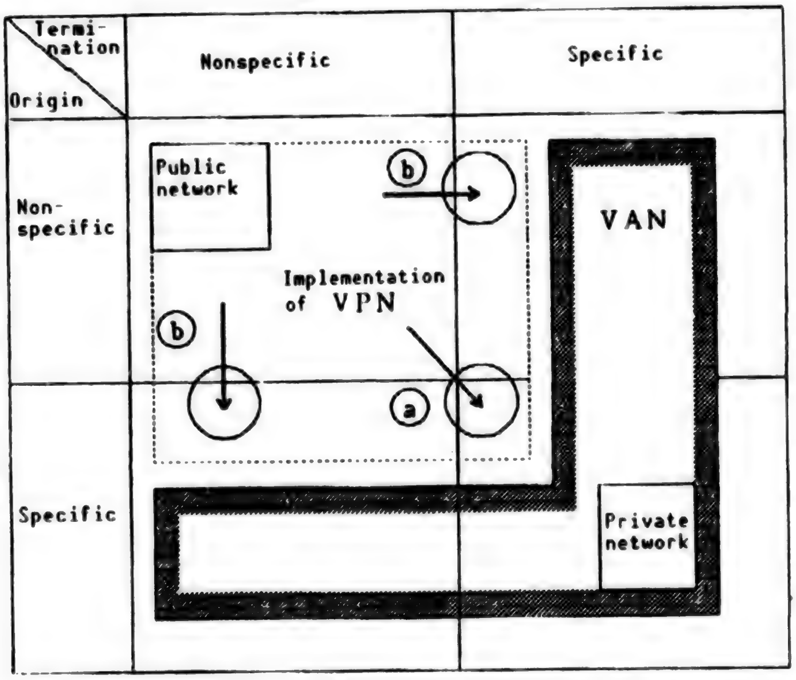


Figure 3.1.2. Relationship Between Terminal Types and Networks

In the previous allotment of functions, the public network was used for communications between nonspecific terminals; VAN was used for communications between nonspecific terminals and specific terminals, or between specific terminals; while private networks were used for communications between specific terminals. The construction of VPNs using the public network does more than expand usage to the area of private networks as a means of communications between specific terminals as shown by (a) in Figure 3.1.2. VAN service suppliers could not construct telecommunications line equipment themselves, so they had to use private lines and public networks with many restrictions as a means of access to user terminals. However, the advent of VPN makes it possible to obtain a means of communication between specific terminals, shown as (a) in Figure 3.1.2, in a form suitable for their purposes, and also to construct the means of communication between specific and nonspecific terminals, shown in (b), in a form suitable for their purposes. This means that, for VAN suppliers, the advent of VPN is equivalent to acquiring the possibility of constructing their own telecommunications line equipment without cost, and it is expected that the impact of this will be very significant for them.

In addition, from the viewpoint of end users, involvement of VAN (VAN + public network) provides the possibility of constructing their own VPNs. From the viewpoint of Type I carriers, it can be expected that they will construct their own VPNs by cooperating with VAN carriers, thereby increasing the added value of the public network. This is expected to be a theme for the future.

3.1.1.2 Unique items for users

In this section, we will list the VPN service items to be made unique, or private, to each user.

(1) Guideline to items to be made unique

(i) Viewpoint of private networks

The development of private networks, which will probably be the largest users of VAN, is expected to follow the pattern shown in Figure 3.1.3.

Private networks have become widely used for the following reasons[1]:

1) Low communications cost.

2) Possibility of ensuring security.

3) Guarantee of line usage (nonblocking, short connection delay, etc.)

4) Possibility of unique network management (unique network configuration, numbering plan, etc.).

5) Excellent affinity with data communications (Digital 1 link, etc.)

6) Possibility of meeting of unique needs.

We believe that it is effective to consider how VPNs should be structured by extending these trends.

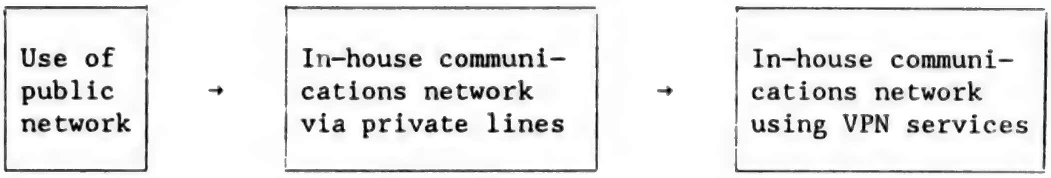

Use of public network
→
In-house communications network via private lines
→
In-house communications network using VPN services

Figure 3.1.3. Form of Development of Private Networks

(ii) Viewpoint of Type II (VAN) carriers

As described in (1) above, for VAN carriers, the use of VPN services will open the way to the construction of access networks suitable for their type of business. In this case, what is required for VPN may include the following:

1) Possibility of preventing illegal access.

2) Possibility of improving the efficiency of usage accounting and billing through, for example levy by proxy.

3) Possibility of organizing a unique charging system, such as a nationwide uniform access charge.

4) Possibility of collecting various management data according to the details of business.

5) Excellent affinity with data communications.

(2) Items to be made unique

Based on the considerations in (i) and (ii) above, the VPN service items that can be made unique are shown in Table 3.1.1.

3.1.1.3 Technical topics

As the architecture of intelligent networks that provide advanced services expand over all networks, such as VPN services, they will require a structure. The structure shown in Figure 3.1.4 is being widely proposed.[2,3] In this architecture, the network consists of switching equipment and transmission equipment. It can be divided into two categories: the transmission layer, which executes services, and the intelligent layer, which characterizes the services that will probably be advanced. The intelligent layer can be further divided into service control, which performs realtime control of individual services according to their specifications, and service management, which assumes nonrealtime management and operations such as data base

Table 3.1.1. Items To Be Made Unique

Category	Items	Importance	
		Private company networks	VAN
Bearer function	Use of ISDN (Provision of Digital 1 link by implementation of VPN on ISDN)	o (5)	@ (5)
Connection control functions	Private numbering plan (Connection by unique numbering system)	@ (4)	
	Closed user group (Restriction of access within or outside the group)	@ (2)	o
	ID check (Checking access right based on ID information before connection)	o (2)	@ (1)
	Route specification (Selection of relay network, selection of satellite link/ground circuit/ etc.)	o (4)	
Quality	Bandwidth guarantee (Nonblocked guarantee of certain band like a private line)	o (1)(3)	
	Connection quality (Unique specification of loss probability, connection delay, transmission delay)	o (3)	
Network management	Network configuration (Setting of unique network configuration)	o (4)	
	Call count (Counting charge of each call based n unique index system)	o (4)	@ (2) (3)
	Management data collection (Collection of traffic data, fault data, etc.)	@ (4)	@ (2) (4)

Importance: @: Very important
o: Important

Note 1: Numbers in circles correspond to the numbers in item (1)-(i).
Note 2: Numbers in circles correspond to the numbers in item (1)-(ii).

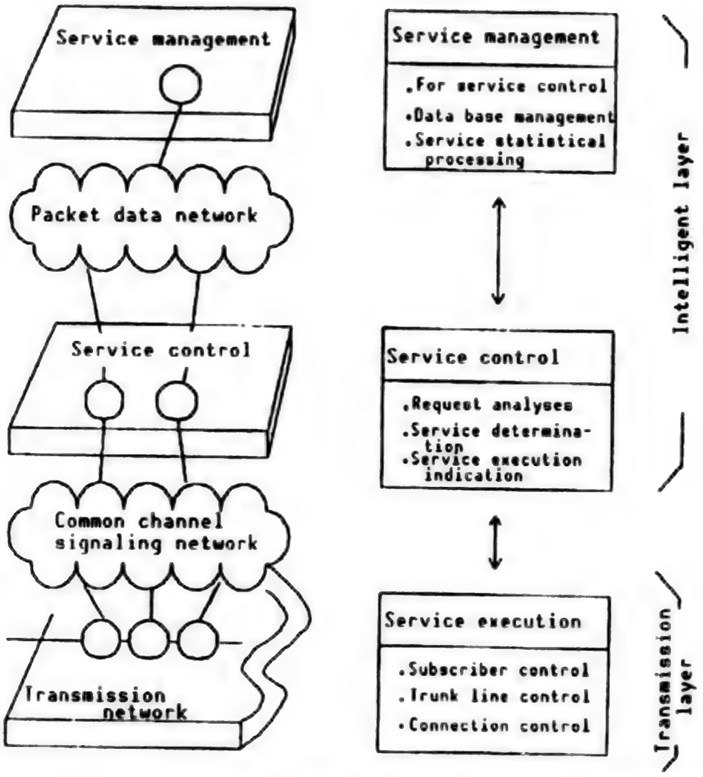


Figure 3.1.4. Intelligent Network Architecture

management and statistical processing. Presupposing this architecture, we will arrange the technical topics to be examined in the implementation of VPN services accordingly.

(1) User interfaces and protocols

The following interfaces should be prepared for interfacing between VPN users and networks:

(i) Service provision interface, for actually receiving services.

(ii) Service management interface, for exchanging the service parameters that make a virtual network unique together with various management information.

Table 3.1.2 shows the protocol plans for these interfaces.

The interface for VAN users can be regarded as the same as the service provision interface for private networks.

Care must be taken along the following lines in interpreting the protocols shown in Table 3.1.2.

Table 3.1.2. VPN User Interfaces

	Service provision interface	Service management interface
Object layers	Layers 1–3	Layers 1–7
Protocol plan	•Analog (majority for the present) •ISDN (28+D, 23B+D) •X.5 packet •X.75 packet •Mobile objects	<Layers 1–3> •ISDN •X.25 packet <Layers 4–7> •OSI management protocol

• The presence of several protocols in one VPN should be possible, in the same way that analog telephones, multifunction telephones and data terminals can be combined as station terminal equipment in conventional private networks.

•Investigations, including assessment of the human interface, should be conducted for high layers of service management interfaces. (For the human interface of network administration, please refer to section 3.4 of the Report for FY 1987.)

(2) Resource management

With the VPN, the users (VPN owners) will secure their own network forms logically while sharing the physical resources of the network. In addition it is also required that the network be capable of responding in realtime to requests from users. This requirement influences overall network resource management. For these purposes, the following technologies should be established quickly in addition to the network design technology, dynamic routing technology and overload control technology that have been developed through experience with public networks.

(i) Technology for providing several service qualities in a network concurrently

Ordinary public networks provide users with services of a common service quality, for example at a loss probability of less than 1/100, etc. But, with VPN, it may become necessary to provide different required qualities according to user needs or to classify the service quality even among the same users.

(ii) Technology to prevent a traffic overload on one VPN from extending to another VPN

Present private networks are constructed on the assumption that they will handle in-company traffic only, and will not be influenced by traffic on the public network or other private networks. Basically, each VPN should be independent from other VPNs with respect to traffic overloads.

(iii) Technology for integrated management of network resources using data bases; technology for on-demand resource reallotment

There are cases in which the guaranteed bandwidth (number of circuits) should be varied dynamically upon request from a user. The VPN should be capable of responding to such requests on demand.

(3) VPN extending across several networks

Following the increasing internationalization of business activities, international networks are being constructed and utilized more than before. MPT research in FY 1987 on 311 major companies showed that 64 percent of them used international data communications and that 41 percent operate systems of their own. Seven companies also started information VAN services.[4]

Naturally, VPN services should also be internationalized. In this case it will be necessary for several VPNs covering national domestic carriers, international carriers and domestic carriers in their companies to work together. There may be several institutional problems, and technical examinations are also necessary into such matters as the method of arranging data bases to match users, protocols for service control signals between networks, protocols for control signals, etc.[5]

3.1.1.4 Trends

(1) International standard[6]

The standardization of intelligent networks, including VPNs, is considered primarily by the CCITT. The CCITT discussed a private numbering plan (CCITT Recommendation 1.255B) in its deliberations on the added service specifications at CCITT SGXVIII in the previous term (1985 to 1988), but the standardization could not be approved as a recommendation because there were too many subjects that required future examination. The examination of standardization is expected to become more active in this term and thereafter.

(2) Present status of VPN[7]

Studies on the practical use of VPNs have been carried out by "VPN" of CNET of France, "SDN" of AT&T in the United States, and by other firms. But VPNs have actually found commercial application only in the United States. Representative examples are shown in Table 3.1.3.[8] The number of users was nearly 300 as of the end of 1987, and the market share is in the order of US Sprint, AT&T and MCI.

These users maintain large-scale private networks and position VPN as a supplementary system to each of the networks. VPN is used mainly for voice services and as a substitute for MTS and WATS for communications with local offices and workshops in distant places based on cost considerations.

Table 3.1.3. Status of VPN Services in the United States

	Service name	Closed numbering connection/subscriber	Public network connection	Network configuration change by user	Administration data provision for user	Architecture
AT&T	SDN	o 7 digits	o	o	o	o Central database (using NCP)
US Sprint	VPN (56k bits/s)	o	o			?
MCI	V Net	o	o			Central database
SBS	SNS (Skyline Network Service)	o	o	x		Distributed databases
US Telecom	VPN	o	o			" "
Western Union	SDNS	o	o			" "
RBOC	PVN	o Within LATA	o			Central database

In the United States, the total annual usage of VPNs is expected to reach 3.5 billion minutes by the end of 1989. This figure is expected to grow at a very high rate over the coming decade as shown in Figure 3.1.5.

3.1.2 Technology of Service Definition by User

In this section, we will describe forms of user-defined networks and examples of user-definable services, and will extract the technical topics to be tackled in the future.

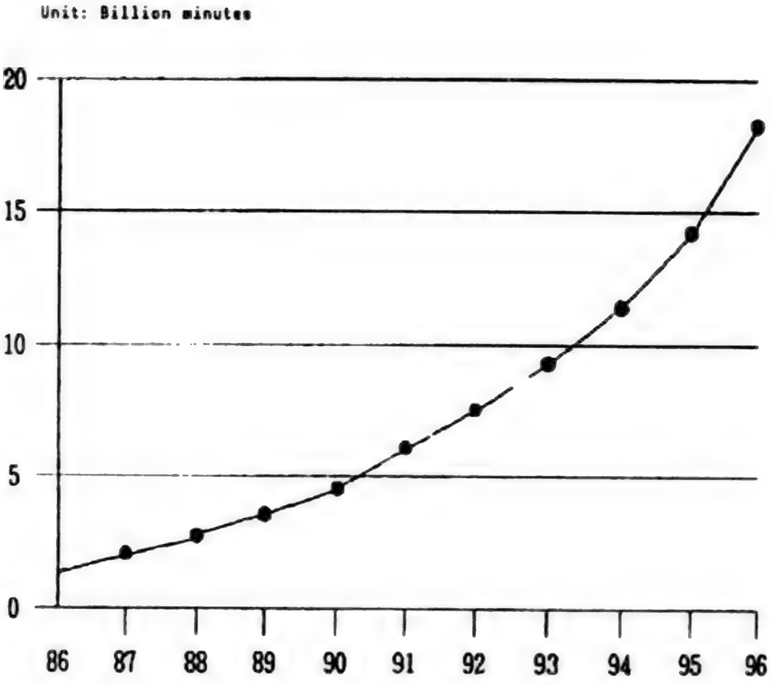


Figure 3.1.5. VPN Traffic (Annual estimated minutes)[7]

3.1.2.1 Forms of user-defined networks

The forms of networks whose services can be defined by users can be categorized into three types, as shown in Table 3.1.4, based on the interfaces opened to users.

(1) Individual-service exclusive interface

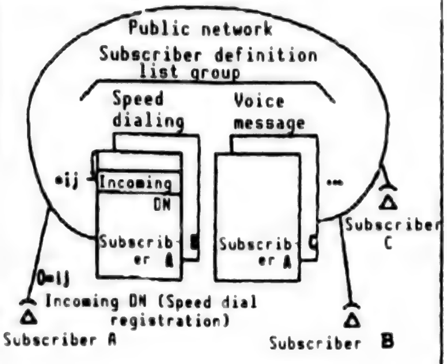
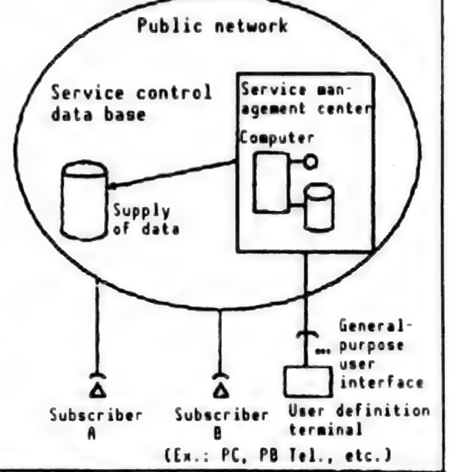
The first form consists of an existing public network where the service provided to users are defined by the users themselves; users can change the data stored in the public network by operating telephone terminals (ordinary touch-tone telephones) connected to the public network. The methods for rewriting data vary depending on the services.

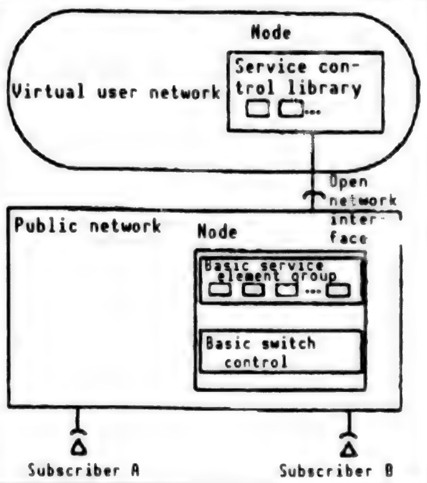
Since users have direct control of data in the public network, this form is limited to only simple services from the viewpoint of reliability. Examples of services include speed dialing and voice message services, which are both defined by user selection from the service menu presented by the public network.

(2) General-purpose user interface

In the second form, a service management center using a general-purpose computer is established in the public network; the center and user terminals are connected via public and private circuits by means of a general-purpose user interface that allows communications with computers, including personal computers; and the service definition information input from user terminals is accepted by the center.[9] After checking the validity of the user-input

Table 3.1.4 Forms of User-Defined Networks

Form name	Existing public network	General-purpose user interface provision network
Outline	 Public network Subscriber definition list group Speed dialing Voice message *ij Incoming DN Subscriber B Subscriber A Subscriber C Subscriber A Subscriber C 0=ij Incoming DN (Speed dial registration) Subscriber A Subscriber B	 Public network Service control data base Service management center Computer Supply of data General-purpose user interface Subscriber A Subscriber B User definition terminal (Ex.: PC, PB Tel., etc.)
Interface	Executive interface for individual service	General-purpose user interface
Services provided	Speed dialing, voice message, etc.	Free dialing, VPN, etc.
Object (users)	General subscribers (general users)	Private company business users, etc.
Defining terminal	Telephone (PB Tel.)	Computer terminals (ex.: PC), telephones (PB Tel.)
Features	.Service menu provided from the public network side .Selection of service on user side .Limited to simple services	.Resource menu provided from public network .Service definition by combining resources .User definition support environment provided in network (Service management center) .Variety of advanced services available by user definition

Form name	Open network interface provision network
Outline	 Node Virtual user network Service control library Open network interface Public network Node Basic service element group Basic switch control Subscriber A Subscriber B
Interface	Open network interface
Services provided	Advanced communications services in general, for example, message reception service
Object (users)	Users, including Type II carriers
Defining terminal	User nodes
Features	.Basic service element functions provided from public network side .Service control by combining element functions on user side .Communications service provision from multiple vendors by publicizing interfaces within public networks .Variety of advanced services available based on the principle of competition

service definition information, the service management center rewrites the data base that controls services in the public network.

In this form, the computer checks the validity of the user's service definition information by means of network simulation, etc., prior to the provision of a service, so that the user can implement advanced services by freely combining communication network resources provided by the public network. Examples of services include free dialing and VPN, and the main users are expected to be private company business users.

(3) Open network interface

With the third form, an interface is defined in terms of the basic element function units (basic service elements) controlling the services in the public network, and this interface is publicized for users as an open network interface.[9] Through this interface, users can implement advanced services by freely combining the element functions provided by the public network. Since this form provides business with opportunities to develop advanced communications services and to offer them to general users, users are expected to be Type II carriers. With the possibility of introducing multiple vendors as advanced communications service suppliers, the development of advanced services based on the principle of competition can be expected.

These three network forms are not contradictory, and there may be cases in which different forms can exist independently or combinations of them may coexist. In reality, it is expected that all of these forms will be combined to form networks that can provide various advanced services.

The extent of advanced services is largely dependent on the service menu, resource menu and service element function menu provided by the public network. Therefore, the primary responsibility for a communication network to respond to social needs may be assumed by the public network.

3.1.2.2 User-definable services

User-definable services are dependent on the service menu, resource menu and service element function menu that can be provided by the public network as described above. However, since advanced services will be implemented in various combinations they will become very numerous. Therefore, the tendency is for the bases of the elements for implementation of the services to be regarded as the objects of user definition and to be provided to users. Table 3.1.5 shows examples of these objects of user definition.

The examples shown in Table 3.1.5 are those with a high probability among existing services. As services based on information processing are introduced in communications in the future, the number of objects is expected to increase.

Typical user-definable services are shown in Table 3.1.6 by taking examples from the extended "800" services of AT&T.

Table 3.1.5. Examples of Objects of User Definition

No.	User definition object	Description
1	Connection condition	The condition for accepting/refusing connection between terminals is the basis for communications, and can be modified temporarily according to the user status. This item enables the user to define this condition.
2	Dial numbering system	This enables the user to have a convenient dial numbering system for the user for use within a closed user system, separately from the dial numbering system of the public network.
3	Resource management	This makes it possible to provide specific lines or service circuits in the public network for the exclusive use of certain users.
4	Connection form	Basically, communications services are implemented by interconnections between terminals, between terminals and lines, or between service circuits. The combinations of connection types will determine the variety of services available.
5	Billing form	Information passes through the communications network in various forms such as voice, data and image. In addition, progress in communications networks is expected to present new services for processing information, and the concept of billing may vary from the conventional concept.

3.1.2.3 Technical themes

In general, it is necessary to impose certain restrictions on user definitions in order to ensure a stable network service quality. Thus network reliability and user definition can be regarded to a degree as contradictory. Therefore, even if a user is able to enjoy custom-made services, whether or not the services are really convenient for the user depends on the extent to which the user can secure the freedom to define network forms and services without disturbing the network and while maintaining it in an operable condition.

Table 3.1.7 shows some of the major technical problems to be solved when implementing a network where user definitions are available.

Table 3.1.6. Extended "800" Services

No.	Name	Contents of services and user definitions
1	Customized call routing	The customer can specify the destination for each call according to the place where it originated.
2	Timer manager	The customer can specify the routing for each time zone in a day.
3	Day manager	The customer can specify the routing for each day in a week.
4	Call allocator	In case several destinations are present, the customer can specify the percentage of calls destined for each.
5	Command routing	In case of an overload or emergency, the custom : can change the routing to a different place by entering a command.
6	Routing control service	The customer can change routing from his or her own terminal without issuing a service order.
7	Call attempt profile	The information on each incoming call can be reported in detail. The format is dependent on the customer's request.

Table 3.1.7. Technical Problems

No.	Theme	Contents
1	Standardization of open interfaces	(1) General-purpose user interface (2) Open network interface
2	Maintenance of normality of user-defined information	(1) User-defined information input method (2) Normality check tests
3	Updating of user defined data bases	Synchronization of centralized and distributed data bases
4	Prevention of influence	

(1) Standardization of open interfaces

The following shows conceivable standardization items for interfaces that the network makes available to users to allow them to define the network services.

(a) General-purpose user interface

For networks providing general-purpose user interfaces, the general-purpose user interface between the service management center, which manages services, and the user-definition terminals in the user's location should be standardized.

The following points are to be considered when standardizing this interface.

(i) Existing user terminals should be serviceable as user-definition terminals

Protocols that have already been used widely as lower-layer protocols--such as the PB telephone interface, the ISDN interface and the X.25 interface--should also be usable.

(ii) The interface should be independent of the services

Given the expandability of services, the application protocols for the higher layers should not be defined on a per service basis, but should be standard protocols independent of the services.

(iii) It should be independent of the network architecture

The user should be able to define services without taking the network architecture and hardware configuration into consideration.

(iv) Security should be ensured

The interface should be able to ensure the security of shared network resources through such techniques as authentication for the correct identification of users, guarding data bases and service control functions, preventing the occupation of common resources, etc.

(b) Open network interface

For networks provided with an open network interface, the network interface between the public network node and the user network node should be standardized.

The following points must be considered when standardizing this interface.

(i) Protocols with small overheads should be used

Since this interface is used every time a service is requested, its protocols should stress the importance of service performance and should be standard OSI or CCITT protocols.

(ii) The basic servicc element functions should be independent of the services

It is desirable that the basic service element functions provided from the public network side, as described in paragraph 3.1.2.1 (3), be made into general-purpose element functions available as part of a number of services defined by users.

(2) Maintenance of normality of user-defined information

One of the important points in service definition by users is how to maintain the normality of service software created by nonspecialists in communications networks.

(a) User-defined information input method[10]

When a user defines a service to suit his or her requirements, the user should give a number of instructions to the network including the service condition specification. A high level of intelligence is required to input these indications correctly. For example, it may be necessary to provide a menu selection system that makes it possible to define services by selecting from the information provided from the network. Or it may be necessary to apply artificial intelligence (AI) processing, which can understand fuzzy indications from the user.

(b) Normality check tests

The following tests should be conducted to check the normality of user-defined services.

(i) Detection of contradictions between user-defined information.
(ii) Check of the convenience to users.
(iii) Evaluation of service performance (delay time).

(3) Preventing existing services from influence[11]

The provision of a new service must not degrade the reliability of the network as a whole.

Also, even when a new service is defective for any reason, it should be possible to provide the services already present without any influence from the defect. To deal with a service that could cause abnormal traffic, for example, it may be necessary to effect continuous monitoring of call occurrence statuses, network resource usage, etc.

(4) Updating of user-defined data bases

For a network provided with a general-purpose user interface, there exists a service control data base for the provision of services in the public network. The service control data base is sometimes concentrated at one location in the network, but several are usually distributed at various locations. There are also cases where data from the same user group are distributed between and managed by several service control circuit boards. In such cases, the problem of how to synchronize updating of the information content of these data bases becomes an important task.

3.2 Network Structure Concealment Technology

In the previous section, we described a VPN that is physically a part of a public network but logically a private network. In this section, we will examine the possibilities and technical requirements for a network configuration that appears physically independent and that does not require users to take the network structure into consideration, taking ATM technology as an example.

3.2.1 Network Concealment in ATM Network

The ISDNs being constructed today can be categorized into wideband ISDNs, which are future networks accommodating image communications, and narrow-band ISDNs with a narrower communications bandwidth. The narrow-band ISDNs provide telephone and data communications with a network access method integrated by one physical and logical interface, thereby concealing the structures of the public telephone network. This network comprises the Public Station Telephone Network (PSTN), the circuit-switched public digital network (CSPDN) and the packet-switched public digital network (PSPDN). When the VPN is provided by a narrow-band ISDN, various voice and data communication services can be provided through a single network so that the user can construct a public network with a certain degree of freedom without being conscious of the network.

The ATM network, which can provide a wide-band ISDN, makes it possible to utilize the features of the ATM described below in addition to the features of a narrow-band ISDN. This can conceal the network structure almost perfectly and further improves the user's convenience, but the network has to overcome a number of different problems to make this possible.

The features of the ATM network and the problems to be solved are as follows:

(1) Communication rates and connection formats

The desired rate of up to 150 megabits/second can be provided by any required form of connection (circuit switching, packet switching, fixed connection, etc.). In addition, they can be set per date, day of the week or even per call at the time of contract. However, for the application of the rate, it is required to define the new rate classification (setting in the units of 64 kilobits/second or setting per each channel such as H1, H2 and H4, or unrestricted, etc.).

(2) Communication bandwidth and hold time

As well as making it possible to set communications at a desired rate, as described in (1), the ATM also allows the rate to be varied during communication or to perform several communications at different rates simultaneously. Since the information on the desired rate is transferred intermittently in the case of packet switching, it can also support so-called burst communications that use the network resources only when instantaneously transferring high-speed data. In this case, however, it is necessary to define the required parameters, including the maximum value and average value, in addition to the rate classification described in (1).

(3) Required quality

The standardization of the service quality is being deliberated by the CCITT. The goal is for the user to be able to set classes of grades (information loss probability, delay time) according to the services and specify the desired class. This will make it possible to continuously secure an existing private line service grade (low error rate, short delay).

On the network side, it is relatively easy to implement class-dependent control by hardware. However, to guarantee the grade requested by the user under any traffic conditions, it is necessary to solve the problem of how to administer the network resources. In particular, while conventional public networks impose restrictions on user requests in case of overloads, the ATM requires new technology that can avoid overloads while meeting user requests. This technology will be discussed in the next section.

While the user has the capability to select the level of service quality according to the application, the user also has to declare the properties (for example, maximum rate, average rate) of the traffic to be applied to the network. Therefore, the user should be provided with a traffic measurement function and a control function so as not to exceed the declared value. On the network side, too, it is necessary to have a function to monitor the declared values and to impose restrictions in case of violations. This is done to protect the service grades of other traffic. Examinations should be undertaken on how to achieve such restrictions by the easiest possible method while improving convenience for both the user and network.

(4) Other

Tariff setting represents an important problem for wider utilization. From the user's point of view, it is desirable to establish a tariff that incorporates more options according to dates, days of the week, time zones, declared rates and connection forms.

3.2.2 Transition to ATM Network

The following are necessary for a smooth transition to an ATM network.

1) To provide existing interfaces at an early stage after installation.

2) To secure communications with terminals in existing networks in later stages.

With regard to 1), existing interfaces should be accommodated by means of terminal adapters (TA) as is done with narrow-band ISDN. For ISDN terminals, which may be installed in large quantities, it may be necessary for the network to be equipped with functions so that the users do not have to prepare a TA.

With regard to 2), it is necessary to guarantee that users can make natural interconnections without any special considerations by providing an optimum gateway on the network side, as seen in the present interconnection between ISDN and telephone networks.

With 1) and 2), users can easily transfer to the new ATM network interfaces as traffic increases.

3.2.3 Self-Recovery Technology

An important theme for network concealment is to establish technology for the self-recovery of network faults without the knowledge of users in order to provide users with a stable service. To date, networks have adopted various methods to ensure stable services. One is to adopt a redundant configuration, which, in case of faults, immediately switches the fault location so that it does not affect the user, thereby maintaining the traffic flow.

By contrast, when temporary overloads occur in a public network, it restricts generating traffic to maintain stability. The requirement for future networks, especially for VPNs, is to be capable of enlarging network throughput in case of overloads to conceal overloads from users. This has to be done by changing the topology of the network to increase the traffic capacity at the desired location. For this purpose, technology for changing the routing according to the date, day of the week and time zone based on previously observed traffic data, by means of variable routing, and for redistributing network resources, is required.

In addition, to deal with unpredictable traffic variations, it will also be necessary to provide technology such as dynamic routing that measures the realtime traffic and immediately varies the routing according to its volume. Such routing technology can be established based on a sufficient understanding of the properties of traffic and on the development of network resource control techniques. Since the ATM network can add the routing information to the transferred information, relatively easy routing control can be expected based on such information.

Together with self-recovery technology, it will also be necessary to provide advanced technology for managing the network quality and resource conditions in order to support the provision of stable services. This technology will be discussed in the next section.

References

1. "Estimation of Demands on In-Company Networks in the United States," DENKIN TSUSHIN, Vol 51 No 504, 1988.

2. Ishikawa, H., "Overall Concepts and Strategies of Evolving Telecommunications Networks," Intelligent Network Workshop, 1988.

3. Hass, R.J., "Intelligent Network/2," ISS '87, A12.1

4. Joho Tsushin Sogo Kenkyujo, JOHO TSUSHIN NENKAN '89, p 54, p 315.

5. Ikeda, Y., "Intelligent Network Capabilities for International Application," Intelligent Network Workshop, 1988.

6. "Final Report to the IXth CCITT Plenary Assembly," CCITT Document AP IX-144.

7. "Features: In-Company Networks in the United States," DENKI TSUSHIN, Vol 51 No 584, 1988.

8. Finan, T., "Software-Defined Network," KAIGAI DENKI TSUSHIN, June 1986.

9. Kamae, N., "Trend of Open Network Architecture (ONA) and Intelligent Networks," COMPUTER AND NETWORK LAN, June 1988.

10. Uchida, et al., "A Study of the Method of Service Definitions by the Users of New Telephone Services," SHINGAKKAI KOUKA KENKYUKAI SE87-8.

11. Takemura, T., "Reliability of Services in an Intelligent Network Environment," Intelligent Network Workshop 1988.

3.3 Telecommunications Management Network

3.3.1 Roles

Progress in telecommunications network features has made the systematic development of management functions necessary. As a result, it has now become necessary to develop a network for the management of telecommunication networks. This is the telecommunication management network (TMN).

There are two reasons for this:

(1) Increased role of network management functions

The form of telecommunications networks has evolved from direct conversations between human beings to conversations between human beings and machines, such as computers, and to information exchanges between machines alone. At the same time, the information is not limited only to voice but now involves multiple media including characters, documents, figures and images. To cope with this, it has become necessary to perform a more detailed management of the administration of information in the network, such as the connection delay, transmission quality, throughput and charges.

Meanwhile, technology for forming virtual private networks (VPNs, etc.) for companies and organizations utilizing public networks is being developed. As it is not desirable for a specific person to be in charge of the administration of this kind of network, the management functions should be automated as far as possible.

For this purpose, it is necessary to develop a system for developing network management functions and for saving as much labor as possible.

(2) Necessity of systematic inversion (and standardization)

The administration of networks, which used to be performed only by one or two specific organizations, is now conducted by many carriers. To provide smooth services through the interconnection of these networks, it is necessary to develop management functions systematically.

3.3.2 International Standardization of TMN

(1) Trend of international standardization

To manage networks characterized by collaboration between human beings and machines, the following details should be defined and implemented by hardware or software.

1) Definition of management system environment: Model, concept, etc.

2) Management purposes (functions): Performance, faults, configuration, accounting, security, etc.

3) Management object identification method: Naming method, management information structure.

4) Management information transfer method: Protocols.

International standardization of TMN is being developed by CCITT SGXV and SG XI. Meanwhile, ISO/IEC JTC1/SC21 has standardized system management functions as a link in its OSI standardization advanced communications. TMN is examined with reference to the situation of OSI management standardization. As for models of concepts, the logical configuration of TMN, which defines the network management elements and interfacing between elements and the summary of functional configurations inside equipment based on OSI, have been defined.

As to the protocols, the protocol for use in the seventh layer (application layer) of OSI is being standardized, and the method of combining protocols in the seven layers is also being standardized. A proposed international standard for a common management information protocol has been created for the former purpose, and the latter standardization is being examined with a view to determining the proper combination of already standardized general-purpose OSI protocols.

Major standardization items and an outline of their development are shown in Table 3.3.1.

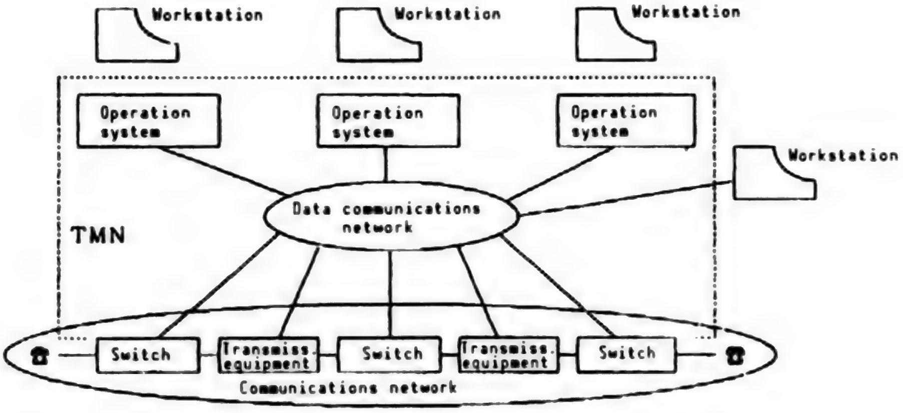


Figure 3.3.1. Positioning of TMN

(2) TMN configuration model

CCITT Recommendation M.30 positions TMN as a network for the management of other networks as shown in Figure 3.3.1. More exactly, the TMN collects data on various management objects for service calls in a network through a data communications network and provides it to the operators of workstations (WS) in various locations. The management objects are selected from the network elements (NE), which are parts of the switching equipment, transmission equipment, etc. according to the required management functions.

Figure 3.3.2 shows an outline of the architecture based on the above. Here the following interfaces are considered:

Q: Interfaces between NE and TMN and inside TMN.
F: Interfaces between TMN and WS.
G: Interface between WS and operators.
X: Interface between TMN and other networks.

(3) Management functions

The OSI defines the concepts of system management and layer management as shown in Figure 3.3.3, and defines the five functions below as system management functions.

1) Performance management: Monitoring of equipment usage rates, traffic, service quality, etc.

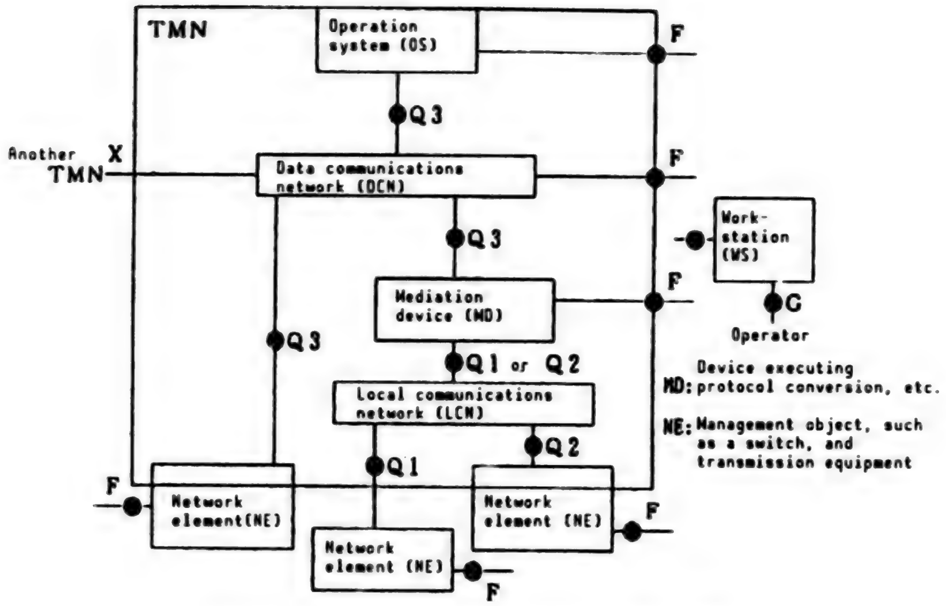

TMN
Operation system (OS)
F
Q3
Another TMN
X
Data communications network (DCN)
F
Work-station (WS)
Q3
F
Mediation device (MD)
G
Operator
Q3
Q1 or Q2
MD: Device executing protocol conversion, etc.
Local communications network (LCN)
NE: Management object, such as a switch, and transmission equipment
Q2
Q1
F
Network element(NE)
Network element (NE)
F
Network element (NE)
F

Figure 3.3.2. Configuration of TMN (Based on CCITT recommendation)

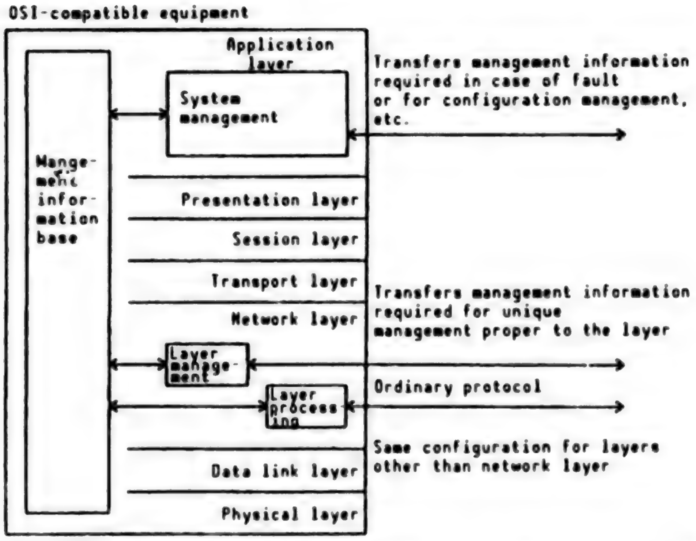

OSI-compatible equipment
Application layer
System management
Transfers management information required in case of fault or for configuration management, etc.
Mange-ment infor-mation base
Presentation layer
Session layer
Transport layer
Network layer
Transfers management information required for unique management proper to the layer
Layer manage-ment
Ordinary protocol
Layer process-ing
Same configuration for layers other than network layer
Data link layer
Physical layer

Figure 3.3.3. Configuration of Equipment in Compliance With OSI (Based on proposed ISO standard)

2) Fault management: Report on alarm occurrences, indication of test executions, report of test results.

3) Configuration management: Modification of equipment connection configuration, monitoring or modification of equipment usage.

4) Accounting management: Notification of billing information.

5) Security management: Management of accesses to various pieces of equipment and to management information.

As it has been determined that the standardization of TMN is to be developed based on the above, what is required for the future is to make their relationship concrete.

(4) The naming of management objects, structure of management information

When executing various management functions, such as the monitoring of alarm occurrences and switching to standby equipment, the unique naming of management objects is necessary for their identification. Names for unique definitions are required for networks and switches, as well as for individual units inside the switching equipment and lines between the switching equipment.

These names are defined according to the network configuration, and the structure for improving the transmission efficiency and reducing the length is being examined.

Next, it is necessary to define the information to be handled according to the details of management functions and management objects. For example, to monitor alarm occurrences, it is necessary to report the fault type, occurrence time, degree of fault, etc., as data. To switch active equipment to standby equipment, it is necessary to indicate the connection relations between equipment after switching. Also, to monitor the traffic status, it is necessary to provide a counter for counting the number of calls on each line or the volume of transferred data. This information is called management information.

The structure of management information is standardized by accumulating various examples of management information and providing common names or configurations for management information types having the same characteristics.

(5) Management protocols

Different types of management information can often be transferred by using a common protocol. For example, an alarm occurrence report and counter value report can be transferred using the same message format designed for reports. Similarly, when indicating various actions to various pieces of equipment, one common message format can be used for different action indications by specifying the contents of the indication through the use of parameters.

The common management information protocol for OSI is based on this idea and implements this function according to the function units shown in Table 3.3.2. For example, reports of alarm occurrence or counter values are transferred using an "event report."

With TMN, the protocols for implementing the above messages are applied for interfacing at points Q in Figure 3.3.1. The following for types of messages may possibly be transferred:

A. Class of management object: Switching equipment, multiplexer, line, etc. (Several tens have been examined.)

Table 3.3.1. Progress of International Standardization (as of June 1988)

Category	Title of standard (Partially abbreviated)	Status of standardization
Model, etc.	Principles for a telecommunications management network	CCITT M.30
	Management framework	ISO/DIS 7498-4
	Systems management overview	ISO work draft
	ISDN user-network interface protocol for management--general aspects	CCITT Q.940*
Management functions	Fault management	ISO work draft
	Configuration management	ISO work draft
	Performance management	ISO work draft
	Accounting management	ISO work draft
	Security management	ISO work draft
	Operations, administration and maintenance application part (OMAP)	CCITT Q.795*
Management object naming method, management information	Structure of management information	ISO work draft
	Generic definitions of management information (GDM)	ISO work draft
Protocols	Common management information service definition	ISO/2nd DP 9595-2
	Common management information protocol	ISO/2nd DP 9596-2
	Q interfaces and associated protocols for transmission equipment in the telecommunication management network (TMN)	CCITT G.771

* The relation with TMN is to be examined in the future.

Table 3.3.2 Functions of Common Management Protocol (According to ISO standard draft)

Function unit	Function outline
Event report (with/without confirmation)	Report generates events to managing system
Linked reply (without confirmation only)	Report results in several blocks to managing system
Get (with confirmation only)	Requests management information value for managed system
Set (with/without confirmation)	Sets management information value for managed system
Action (with/without confirmation)	Indicates management action to managed system
Create (with confirmation only)	Instructs creation of management object to managed system
Delete (with confirmation only)	Instructs deletion of management object to managed system

B. Attribute of management object: Active/standby, number of error packets, etc. (Status or characteristic of object.)

C. Event: Fault, switching, etc. (Information occurring in the object controlled, which should be transferred to other equipment.)

D. Action: Test, etc. (Processing series to be executed by the management object.)

3.2.3 Future Topics

(1) Promotion of domestic standardization

The standardization of TMN and the standardization of the OSI management system are critical for the systematic construction of information networks, but in Japan their examination is proceeding slowly at present. Beginning now, concrete measures must be taken to ensure the efficient promotion of domestic standards, focusing in particular on applications in the public network, VPNs, etc. The important objects include the interfaces at points X, F and G in Figure 3.3.2 as well as the interface at points Q.

(2) Topics in view of implementation

A concrete examination of the development of hardware and software design is necessary in conjunction with the application of OSI common management information protocols to TMN. For example, when monitoring alarm occurrence, it is necessary to select the fault report function included in the fault management function, and provide a physical meaning, such as circuit break, as the type of fault to be reported.

(3) Research topics

The decision to switch to standby equipment in the case of a fault requires processing, including the estimation of faulty equipment based on the alarm information. For this, it is necessary to investigate the application of AI technology, focusing on export systems.

References

1. Morino, Tanaka and Matsushita, "OSI Protocols for Network Management," NTT SHISETSU, Vol 40 No 8, August 1988, pp 21-24.

Chapter 4. Measures for Utilization of AI Technology in Advanced Communication Networks

4.1 Present Status of AI Technology, Its Application in Communication Networks

We shall examine the most urgent and important problems among the technical themes related to advanced communications pointed out in FY 1987, and outline a system designed to tackle them.

In this chapter, we will examine the role of artificial intelligence (AI) technology, which is one of the most important basic technologies supporting the development of networking. We will also clarify a number of technical development problems that must be solved in connection with the achievement of advanced communications.

In other words, assuming an advanced communications network configuration that has an intelligent and flexible structure for both carriers and users, we will describe the concept of a user-defined networks and the technical themes to be used when providing intelligent features to networks. Also, we will examine problems related to the introduction of AI technology in network design, administration and maintenance, and security.

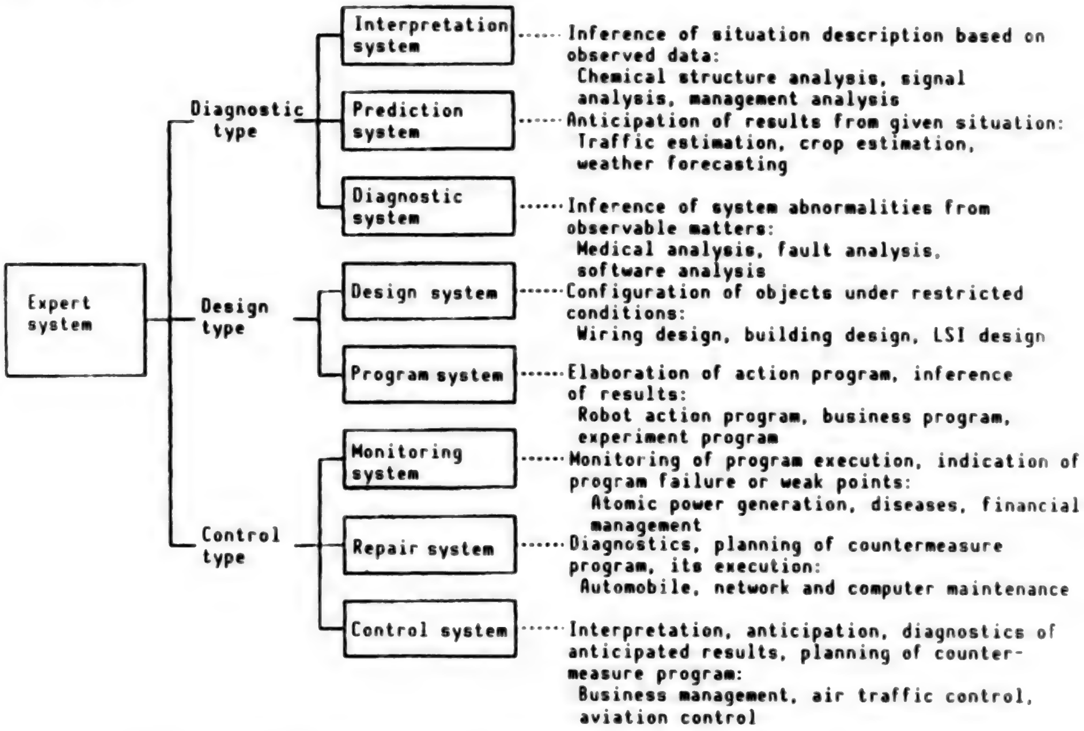
4.1.1 Trends in AI Technology

AI has long been a subject of fundamental research. Since knowledge engineering was first proposed by A. Feigenbaum in 1977 and with the start of the fifth-generation computer project in 1982, AI has attracted worldwide attention and it is actively being researched as a frontier information processing field. As the results start to be put to practical use and commercialized, it is expected that it will show high growth in the future.

Modeled on the intelligent functions of the human brain, such as knowledge and thinking, AI is an attempt to implement similar functions mechanically. At the same time, knowledge information processing is also an attempt, based on the achievements of AI research, to turn the intelligent functions into algorithms that can be handled by computers and to systematize them so that they can be used in solving various problems.

Increasing the efficiency of intelligent production activities, planning, design, administration, management and the maintenance of systems that are becoming ever larger and more complicated due to the diversification of needs will become important tasks in a future advanced information society. These matters have previously been handled by human beings who have expert knowledge. But, due to the problems involved in acquiring the necessary experts, handling the knowledge and improving the efficiency, it is expected that their knowledge will be handed over to expert systems.

An expert system can be defined as a computer system in which the knowledge of experts and past data are stored in the form of a knowledge data base, which has an inference function described in a language such as PROLOG, and which plays the role of an advisor in judging responses to various phenomena. Expert systems are expected to be built in order to deal with various problems (Figure 4.1.1).


Expert system
Diagnostic type
Design type
Control type
Interpretation system
Prediction system
Diagnostic system
Design system
Program system
Monitoring system
Repair system
Control system
Inference of situation description based on observed data:
Chemical structure analysis, signal analysis, management analysis
Anticipation of results from given situation:
Traffic estimation, crop estimation, weather forecasting
Inference of system abnormalities from observable matters:
Medical analysis, fault analysis, software analysis
Configuration of objects under restricted conditions:
Wiring design, building design, LSI design
Elaboration of action program, inference of results:
Robot action program, business program, experiment program
Monitoring of program execution, indication of program failure or weak points:
Atomic power generation, diseases, financial management
Diagnostics, planning of countermeasure program, its execution:
Automobile, network and computer maintenance
Interpretation, anticipation, diagnostics of anticipated results, planning of countermeasure program:
Business management, air traffic control, aviation control

Source : Hayes-Roth, F., et al., "Building Expert Systems," 1985

Figure 4.1.1. Categorization of Expert Systems

As the hardware for information communication systems is coming on line, centralized processing is being replaced by distributed processing in which information is processed at each of its sources. In the course of processing, it is necessary to handle various media in addition to numbers and characters, such as voice, natural languages, diagrams and images.

The majority of these processing operations are performed by software. Thus software is becoming more complicated and larger in size, and increasing software productivity has become an important theme. Also, most of the steadily increasing nonprogrammed processing does not use explicit algorithms but requires knowledge and inferences achieved through trial and error. Thus the introduction of knowledge information processing has become unavoidable.

In other complex fields, the ability to understand voices and natural languages, the recognition of figures and images, and increasing productivity, software, expectations for advanced processing based on inference and knowledge are becoming very high as well.

Meanwhile, the price of computers has fallen drastically thanks to the rapid progress in the development of semiconductors. A higher degree of functionality and higher level of performance have become possible as well. With regard to computer architecture, non-Von Neumann-type architectures and various parallel processing systems are being proposed to replace Von Neumann-type serial processing.

As the result of extensive research into AI, LISP and PROLOG were developed as languages suitable for knowledge information processing. Frameworks for expert systems involving knowledge expressions and intelligent search techniques have also been proposed, and their effectiveness has been confirmed in practice.

Meanwhile, the fifth-generation computer project is currently involved in research into a wide range of knowledge information processing technologies.

AI and knowledge information processing are attracting notice in terms of both "needs and seeds," and active research is being conducted worldwide, including a search for practical applications. Based on these results, commercialization is expanding rapidly.

4.1.2 Application of AI Technology in Networks

This section deals with the direction in which future communications should proceed, the role of AI technology in advanced networks, and the relationship between communications and AI and knowledge information processing.

Information communications are expected to make great progress and undergo a remarkable transfiguration in the future. Consequently, the roles of AI and knowledge information processing technologies will be keys to unlocking this future.

These technologies are still in the development stage, and further fundamental research is required. But some of the fields, such as expert systems, have reached the point where they can actually begin to be applied.

Considering the future direction of networks, it is expected that various themes will emerge following the development of ISDNs, their standardization, and the start of ISDN services.

For the construction of complicated advanced communications networks and their efficient management and administration, the application of AI technology, in which rapid progress is being made, will be very effective.

Therefore, it is anticipated that future services may not be the same as conventional telephone or telex systems in which carriers provide all services up to the terminals, but may be configured so that new kinds of terminals, computers and private networks can use public networks freely while public networks themselves can provide a variety of services.

In such a system, the network is expected to evolve from a simple means of providing the transmission paths to the source of information network services, while network utility services will be freely available to users.

Since providing the network with intelligence is indispensable for such an evolution, it will be necessary to provide a higher level of functions to the interfacing equipment between the network and terminals and to the switching equipment itself. It will also be necessary to introduce a network host, such as the network service center.

In the development of communication networks from ISDNs to wide-band ISDNs and intelligent communication networks, communication networks may advance and be made intelligent by the gradual introduction of AI technology.

4.1.3 Provision of More Advanced Services and AI

The provision of more advanced services means the implementation of services that are aimed at improving user convenience. To activate communications in the current method, the user has to remember the correct telephone number or access code. This means that the user has to perform a dialing operation according to the requirements of the communications system, and thus the user is forced to perform operations that have nothing to do with his or her original intention.

It is desirable that future intelligent communication systems will allow the user to transfer information with the same ease of communicating with another human being.

To make such a communications system possible, it may be important to arrange and systematize various pieces of knowledge related to communications by introducing logical numbering, for example, and to apply knowledge information processing so that a person's intentions can be understood and executed correctly.

Human interface technology and directory systems may form the core of this effort.

As communication systems develop under human initiative, the relationship between communications and AI will be closer than ever, and R&D into this subject should be conducted more positively.

Going even further than the above, machine translation between different languages and automatic translation telephones are also important subjects that could solve the problem of understanding between different parties, which is the essence of communication. It is necessary to conduct priority R&D in these subjects as well.

4.2 AI Support Technology Used in Network Design

By applying AI in the technology used to support complicated knowledge related to network design by using a knowledge base for building advanced communications networks--which is also in demand for estimation and design know-how--detailed designs that meet various needs become possible.

For expert systems to manage communication networks, an application of AI technology may be used together with TMN, as described in Chapter 3.

4.2.1 Trends of Network Design Support Technology

Some support systems incorporating various tools required in public network and company network design have already been put to practical use. To establish design technology for networks that are becoming more advanced and complicated, as illustrated by ISDN, it is necessary to develop network design support systems by integrating the administration methods of routing, etc., and connection quality control methods based on the need for alternative routing and on the kinds of services to be provided.

4.2.2 Application of AI Technology in Network Design Support

Individual conventional networks have been built according to their voice or data applications. Now, the task is to integrate them into more efficient, lower-cost digital networks. In this regard, communications involving symbols, voice and images are being integrated into one network within a company or company group.

To allow the construction, enlargement and development of such networks, it is necessary to make network system design possible even by less experienced engineers. This means that the relationships between the constituent elements and the basic data determining them, or between several elements, has to be clarified further.

It is also necessary to show the guidelines and reference for the design procedures by clarifying the required work steps and work items early in the design stage. This makes it possible to systematize and standardize design work and facilitates the introduction of AI technology.

It is desirable to implement an expert system that can support design work based on various kinds of knowledge related to communications system design, and an expert system that can facilitate automatic software design based on knowledge of software production. Another desirable expert system is a network design expert system for use in customer consultation, equipped with a user-friendly interface.

Some systems using AI technology in network design have, in fact, already been implemented or are being used as trial systems. Support tools for optimum network design that take into account, for example, the cost, extent of services, reliability, traffic and communication protocols, are already being used to some extent.

This kind of system accepts the input of a wide range of design information including office location information, host information, terminal information, communications line information (private line and public line usage conditions, etc.), communication rate, transmission efficiency, response time, etc., and outputs the network diagram, cost, etc. In addition to the flexible arrangement of network design tools that meet the conditions for network expansion and the addition and displacement accompanying changes in the business environment, the incorporation of the knowledge of many experts in the form of tools is also desirable.

4.3 AI Support Technology Used in Network Management and Administration

4.3.1 Trend of Network Management Technology

Many business or company networks are being built as a result of the liberalization of communications and increased use of low-cost high-speed digital lines. Following this, an increasing number of companies are installing "network management systems" to support their network administration.

The network management systems for the present may consist of administration and management systems performing centralized management of communications equipment, or systems performing a quantitative evaluation of networks using models based on the control effect evaluation program of various traffic control equipment and on several other factors such as network cost and reliability. The functions managed include the operating status, fault points and details, equipment configuration, diagnostics and switching.

In the future, these systems are expected to give way to systems that can output performance evaluations or expansion plans for the whole network in realtime based on interlocking arrangement with a large-scale traffic data base, office information, or other data bases possessed by the network management system.

4.3.2 Application of AI Technology in Network Management Technology

The network management system refers to tools for supporting the wide variety of jobs associated with network administration, especially the administration, maintenance and management of facilities. It is anticipated that the relationship between network management and AI technology will consist of reinforcement and progress based on connections with various kinds of information related to the network.

At present, network management systems are changing from systems that control individual pieces of network component equipment (modems, circuit switch equipment, packet switching equipment, etc.) to integrated network management systems in which these individual equipment management systems are connected organically by means of communication lines. This change is oriented toward creating more efficient systems through the centralized management of all network component equipment.

The CCITT is now standardizing a telecommunications management network (TMN) which manages the equipment by collecting maintenance and administrative data. The TMN interface allows users to collect the network maintenance and administrative data and dynamically control the parameters of the network.

Such network management systems make it possible to collect various pieces of information from network component equipment and to perform that centralized control. This will improve the efficiency of routine jobs such as equipment administration and maintenance. Meanwhile, the determination of faults and the selection of countermeasures are expected to be commissioned to experts and supported by AI technology, that is, by expert systems.

The application of expert systems in network management systems is still at the examination stage, but in-company experiments using prototypes are already being conducted with respect to switch fault diagnostics, etc.

In the United States, the "ACE" fault analysis expert system for the in-company cable facilities at Bell Laboratories is already in practical use, and the "COMPASS" switch malfunction diagnostic and analysis system at the GTE Laboratory is undergoing on-site testing. At BBN, the "DESIGNET" network design support tool is already being used by the company as a consultation support tool. There are also some expert systems for use in network administration that are in the development stage.

Since the network management system itself is a support tool, cost efficiency must be taken into consideration at the time of its installation. As networks are becoming larger and more sophisticated, it is anticipated that the importance of AI technology will further increase and that AI technology will be established that can be used in network management systems by utilizing knowledge bases, etc.

It is thought for the present that network management systems can be enhanced functionally by accommodating security and customer-controlled configuration functions. But these functions may be further enhanced by the use of expert systems.

The ultimate network management structure may be the integrated control of several networks. Because the method of intersystem utilization of management information in individual networks and the range of their publication may pose problems, it is necessary to ensure that the security of management information is sufficiently accounted for.

4.4 AI Support Technology Used in Network Maintenance

4.4.1 Trends of Network Maintenance Technology

Meanwhile, communications systems are entering an age in which advanced functions are being implemented to meet the diversification of needs. Because of the enormous growth and complexity of communication systems, their administration and maintenance are now almost beyond human capabilities.

As a result of the enormous growth and sophistication of communication systems, the desigr, administration and maintenance of communications and the development of associated software can no longer be conducted manually. Consequently, it is becoming mandatory that these operations be partially or fully automated with the support of computers.

4.4.2 Application of AI Technology in Network Maintenance

To solve these problems, it would be best to implement an expert system in which the knowledge of experts who have been in charge of maintenance and administration is stored as the knowledge base. The system would then be able to infer faulty locations and execute optimum measures to correct them.

In concrete terms, R&D into expert systems that can perform diagnostics and consultations for communications protocols for the users of ISDNs, etc., will be important. The development of automatic answering systems utilizing voice recognition technology is also expected.

To minimize trouble in actual administration, which occurs when detecting the location of a fault in communications equipment or when isolating faults, R&D into diagnostic expert systems utilizing the experience of maintenance personnel in its knowledge base is also in progress.

Research is also being conducted into intelligent support technology that should provide operators with a user-friendly interface.

With respect to the application of AI technology in network maintenance, equipment fault analysis expert systems, automatic administration expert systems, and man-machine interface (MMI) expert systems will be developed on a priority basis in order to improve routine jobs, such as reducing maintenance and speeding up trouble processing.

4.5 Future Themes

It is anticipated that the following technical themes associated with the application of expert systems in network design, management and maintenance will also be pursued:

(1) Development of practical uses interface

It is necessary to examine an easy-to-use interface and how to incorporate expert systems in an existing network management system.

(2) Collection of data, arrangement of knowledge

Data should be input so that an expert system can run the inference function (for example, fault messages from the object being managed are necessary in a fault analysis expert system). It is necessary to determine how to collect sufficient data from various object equipment, possibly from multiple vendors, and how to arrange this systematically.

(3) Advancement of knowledge base

The expert systems already completed are still not sufficient, compared to the thought processes of human beings, and their knowledge bases must be improved. Therefore, it is necessary to examine the method by which the technology for acquisition, expression and utilization of knowledge is to progress.

(4) Development of voice recognition/natural language understanding technology

It is necessary to develop or enhance the technology mandatory for building expert systems with a user-friendly or man-machine interface (for example, voice recognition/natural language understanding technology) as soon as possible.

(5) Training of knowledge engineers

It is necessary to train knowledge engineers (KE) who understand both network technology and the AI technology to be used with the fundamental facilities in order to introduce AI technology effectively.

Meanwhile, with respect to advanced communications technology related to the processors constituting communication nodes, support equipment and service machines, research is being conducted into the configuration of high-speed, wide-band processing equipment, especially the construction of parallel processing equipment, large-capacity data base machines featuring high-speed inquiry functions, fifth-generation computers approaching AI, and neurocomputers that can simulate the neural circuits of living things. Although they are at present in the fundamental research stage, their impact will be very great when they are implemented.

References

1. "Technical Problems Related to the Introduction of Artificial Intelligence Technology in the Telecommunications Field," DENKI GIJUTSU SHINGIKAI, 1988.

2. "Information Network Features," DENSHI JOU-SHIN-SHI, Vol 70 No 11, 1987.

Chapter 5. Security Technology in Advanced Communications Networks

5.1 Trends of Standardization

5.1.1 Systematization of Security Technology

In a broad content, security technology can include technical measures against nonintentional threats, such as natural disasters and mistakes. But if we focus on intentional threats, we can enumerate authentication technology, access control technology, isolation technology and monitoring technology as combining to form what is currently defined as security technology. Although this categorization was presented in the report for FY 1987, we list it again in Table 5.1.1 because it represents the background for discussions conducted since FY 1987.

Table 5.1.1. Categories of Security Technology

Category	Contents	Concrete countermeasure technology
Authentication	User authentication	
	Knowledge utilization	Password
	Authentication of possession	Magnetic card, IC card
	Authentication of personal attributes	Fingerprint, voiceprint, retina pattern combination
	Message authentication (alteration detection)	Cipher feedback method
	Digital signature (assurance of origin)	Unidirectional function, application of public-key encryption
	Originating terminal authentication	Call back
Access control	Maintenance of access right information by accessed party	Competence list
	Maintenance of access right information by accessing party	Capability list
	Prevention of analogy of information of statistics data base	Inference control: Question breakdown method tracker method linear simultaneous equation method

[continued]

[Continuation of Table 5.1.1]

Category	Contents	Concrete countermeasure technology
Isolation	Isolation control between processes by OS	Ring level, virtual space
	Encryption-related technology	Customary key encryption (DES, etc.), public key encryption (RSA, etc.)
Monitoring	Input data recording	Logging

5.1.2 Trends in Encryption Technology and International Standardization

Encryption technology is an important technical element of security technology. It is not only the core of isolation technology, but also is utilized widely in authentication technology.

Encryption technology can be generally classified into two categories: traditional encryption technology and public key encryption technology.

(1) Traditional encryption technology

There are two types of traditional encryption technology: systems in which the encryption algorithms are made public and systems in which they are not made public.

Examples of public algorithm technology include the DES (data encryption standard) established as the U.S. standard in 1977 and the FEAL (fast data encipherment algorithm) developed in Japan. Both are block encryption systems that can transform a 64-bit normal text (or encrypted text) into a 64-bit encrypted test (or normal text).

ISO/IEC JTC1/SC20, which has been examining the standardization of encryption-related technology, has stopped the standardization of encryption algorithms themselves. However, the utilization modes of the block encryption system have already been standardized.

These systems use a structure in which the block cipher output is fed back. It has three modes: CBC (cipher block chaining), CFG (cipher feedback) and OFB (output feedback). CFG and OFB were standardized in IS 8372.

The best-known customary encryption technology with a nonpublic algorithm is NLFSR (nonlinear feedback shift register), which handles bit information in the form of streams. It is called a stream encryption system. Here, the algorithm for generating nonlinear random information is kept confidential.

In traditional encryption, the technology for safe delivery of a common secret key between the sender and receiver of encrypted communications is being examined. In this technology, there is a method called the hierarchical key system, in which the key for encrypting information (data encryption key) is encrypted using a second key (key delivery key6), which has been held in a certain way, and then delivered. ISO/TC68, which is responsible for the standardization of banking jobs, is developing standardization for a system that uses two key delivery keys (DIS 8732). Meanwhile, the MPT has proposed a system for delivering the data encryption key by using a public key encryption system.

(2) Public key encryption technology

Public key encryption systems are constructed using a function that is unidirectional in terms of the calculations performed. Such unidirectional functions include prime factorization (although it is easy to calculate n = pq from primes p and q, it is difficult to obtain p and q from n) and discrete logarithms. The former is used in the ERSA encryption system, while the latter is used in the Elgamal encryption system.

Public key encryption technology is a very effective means for secret communications via public networks. Its use makes it possible to implement a digital signature function (confirmation of the validity of the transmitter, confirmation of the absence of alterations in transmitted messages).

5.1.3 Themes for Standardization

There is a growing possibility that an "inconvenience" (for example, a fault or illegality) in the information communications network will spread throughout the network or throughout society. Several arguments have been developed over the standardization of security technology, and the standardization of encryption itself has not shown much progress. Here, we will discuss standardization trends in the framework of OSI (open system interconnection), which makes communications between different computer models possible.

(1) ISO/IEC JTC1 SC20

SC21 deals with standardization related to OSI, and it has standardized security architecture as Part 2 (IS 7498/2) of the OSSI Basic Reference Model (IS 7498). The IS 7498/2 standard defines data confidentiality data integrity, access control, peer entity authentication, etc., as security services to be used in OSI layers, and has positional encryption, as the appropriate technology for executing these services.

Meanwhile, SC21/WG4, which is examining OSI management, also covers the management and delivery of encryption keys for items being examined. The OSI Directory Service (IS 9594) also deals with authentication, and it is standardized as IS 9594/8.

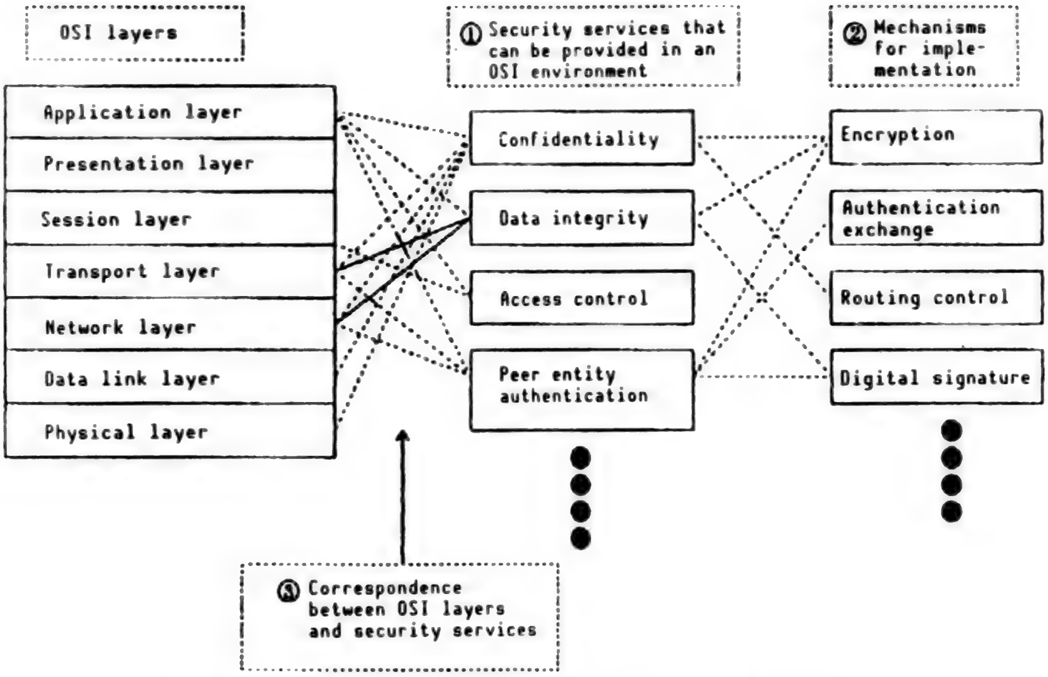


Figure 5.1.1. Standardization Work Related to Security Architecture

The security packaging method for each layer related to OSI has also been examined. The higher layers are the responsibility of SC21/WG6, and the lower layers are the responsibility of the SG6/WG4.

As the importance of security technology in information communications grows, efforts are underway to examine the framework of security technology from a more general point of view that is not limited to OSI.

The result of this work is scheduled to be issued as a standard consisting of the following seven parts:

Part 0:	Outline (specification of common concepts and framework for security)
Part 1:	Framework for authentication
Part 2:	Framework for access control
Part 3:	Framework for repudiation assurance
Part 4:	Framework for integrity
Part 5:	Framework for confidentiality
Part 6:	Framework for audit

These are developments of the previous IS 7498/2 standard, and their purpose is to make it possible to carry out general operations across several domains. Parts 0 to 2 are currently being given priority.

The security architecture examined by ISO/TC97/SC21 is being standardized as a security function that is an important constituent element of network architecture.

Securing architecture is the concept that clarifies the principles and functional structure for safe information transfer in an OSI environment. In other words,the mechanisms for implementing the security services and safe data transfer, and the positioning of these services and mechanisms in the OSI reference model are being examined.

The details of security architecture define the concepts of how to implement security services in OSI for system interconnections.

5.1.4 Standardization Work Related to Security of OSI

The security standardization work of OSI is conducted by the ISO.

(1) ISO TC97/SC21/WG1

Here the concepts of security services in an OSI communications environment called security architecture are examined.

Security architecture is a conceptual collection of security services to assure safe information transfer between open systems in an OSI environment, and mechanisms to assure the implementation of these services.

The details of the standardization work related to security architecture are as follows:

1) Extraction of security service concepts under OSI

Security or confidentiality services that can be provided in an OSI environment (for example, information security or confidentiality services and a service/data alteration detection service using encryption) are extracted and compiled.

2) Mechanisms for implementing security services

The mechanisms required to implement security services extracted in 1) above are arranged, and their relationships and areas of overlap are clarified.

3) Correspondence between 1) and 2) above and OSI communication function layers

In addition, it is necessary to identify those OSI reference model layers where the security services and their implementation mechanisms can be applied. For example, connection-type security (confidentiality) services using encryption can be applied to the physical layer, link layer, network layer, transport layer and application layer.

(2) ISO TC97/SC20/WG3

Here, a concrete examination of means for the actual implementation of security services is developed. (Specific topics discussed here include ways to implement the security of confidentiality service in the transport layer;

a method of setting detailed encryption parameters, such as the encryption algorithm and encryption key; and negotiation procedures.)

5.1.5 Security Services

Security services are indispensable elements for the construction of future information communication networks.

The security services provided in the framework of the OSI reference model are as follows:

(1) Authentication

(1.1) Peer entity authentication

This service makes it possible for one entity to authenticate the identity of another entity among peer entities in the object layer. It is applied at the time of connection establishment or data transfer for the purpose of preventing "camouflage" (disguise) or replay (illegitimate reuse) by an illegal system.

(1.2) Data origin authentication

This service ensures that the data in connectionless-type transmission is transmitted from a valid peer entity (however, it cannot assure the superimposition of data units).

(2) Access control

This service prevents illegal access to OSI resources. It is applied to various types of access including the utilization of communications resources, the read/write/deletion of information resources, the execution of information processing resources, etc.

(3) Data confidentiality

This covers security or confidentiality services that prevent illegal exposure (leakage of data, and includes the following:

(3.1) Connection confidentiality

This makes all of (N) user data units on (N) connections confidential. However, depending on utilization forms and layers, it is sometimes difficult to make all data confidential, such as priority data and all data in a connection request.

(3.2) Connectionless confidentiality

In connectionless-type transmission, this makes all of (N) user data in the form of single (N)-SDUs (service data units) confidential.

(3.3) Selective field confidentiality

This makes (N) user data or (N) connections, or selective fields contained in (N) SDUs of connectionless transmission confidential.

(3.4) Traffic flow confidentiality

This makes it impossible to acquire unauthorized information by observing traffic flow (direction, flow amount, frequency, etc.).

(4) Data integrity

These services check for the intentional or nonintentional alteration of data sequences.

(4.1) Connection integrity with recovery

This assures the integrity of (N)-user data on (N)-connections by detecting alterations, insertions, replays, etc., of SDU sequences and recovering them as required.

(4.2) Connection integrity without recovery

This is the same as (4.1) above except that the recovery processing is not executed.

(4.3) Selective field connection integrity

This assures the integrity of selective fields in the (N)-user data on (N)-SDUs transferred on the connections; this is done by detecting alterations, insertions, replays, etc. in the selective fields.

(4.4) Connectionless integrity

This assures the data integrity of single (N)-SDUs transmitted by a connectionless-type transmission by detecting alterations of received SDUs.

(4.5) Selective field connectionless integrity

This assures data integrity in selective fields of single SDUs transmitted by a connectionless-type transmission by detecting alterations.

(5) Nonrepudiation

(5.1) Nonrepudiation with proof of origin

Proof of data origination is provided to the data receiver. This prevents the sender from repudiating the sending of the data or the contents transmitted.

(5.2) Nonrepudiation with proof of delivery

A proof of data delivery is provided to the data sender. This prevents the receiver from repudiating the reception of the data or the contents received.

5.1.6 Security mechanisms

Security services are provided through the following mechanisms:

(1) Encryption

An encryption service is provided to conceal information related to data and traffic flow; this mechanism is often used in combination with other security mechanisms.

The encryption algorithms include the following:

- Symmetrical (nonpublic key) encryption
- Asymmetrical (public key) encryption

(2) Digital signature mechanism

The digital signature mechanism deals with signature processing and inspection processing. Signature processing uses the private information possessed by the signatory, such as the secret key, to encipher data units, etc. The inspection processing deciphers the signed text using a public key and checks to confirm that it was generated by the signatory.

(3) Access control mechanism

This mechanism determines the resource access right or executes the access using information certifying the identity of the entity seeking access. Illegal access to resources is rejected and the rejection is notified. Access control is performed based on the following information:

- Access control information (information on the access right of peer entities)
- Authentication information (password, etc.)
- Capability
- Security level
- Access time, access period, access path, etc.

(4) Data integrity mechanisms

Data integrity includes the integrity of data units themselves and the integrity of "streams" of data units. Different mechanisms are used for them.

First, to ensure the integrity of the data units themselves, the sending side marks additional information, such as a block check code, and the receiving side checks to see if alterations have been made during transfer. If any alteration is detected, the required recovery processing is performed in that layer or in a higher layer.

With connection-type data transfer, it is necessary to mark the sequence numbers or use a time stamp to assure the integrity of the sequence of data units. Marking with a time stamp will be required in the case of connectionless-type data transmission.

(5) Authentication exchange

This assures one party of the identity of the other. The following methods are used:

- Utilization of information related to authentication, such as passwords.
- Encryption technology (the use of a handshake protocol may be applicable to replay).
- Utilization of the characteristics and possessions of the entity.

This mechanism is incorporated in layer (N) in case the authentication of (N+1) peer entity is required. If the authentication does not end successfully, the connection may be refused or released.

(6) Traffic padding mechanism

This mechanism transmits false data units or other signals to prevent the traffic from being analyzed. It presupposes the use of data confidentiality services.

(7) Routing control mechanism

This mechanism selects routing dynamically or according to the previous setting by using a physically safe subnetwork. For example, when an alteration is detected on a route, the transmission is shifted to another route.

(8) Notarization mechanism

The notarization mechanism is used by a third party (notary) who is commissioned by the communicating entities (sender/receiver) to confirm the chara teristics related to their communications, including data integrity, origin and time.

For this purpose, high-reliability channels backed up by the digital signature, encryption and data integrity service cannot the notary to the sender and receiver, and data is exchanged via the notary.

Figure 5.1.2 shows which security services are implemented by what kinds of security mechanisms, and in which layers of the OSI reference model these services can be positioned.

Mechanisms										Layers						
Encryption	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization	Services		1	2	3	4	5	6	7*1
○	○			○				Peer-entity authentication		—	—	○	○	—	—	○
○	○							Data origin authentication		—	—	○	○	—	—	○
		○						Access control		—	—	○	○	—	—	○
○						○		Connection confidentiality		○	○	○	○	—	—	○
○						○		Connectionless confidentiality		—	○	○	○	—	—	○
○								Selective field confidentiality		—	—	—	—	—	—	○
○					○	○		Traffic flow confidentiality		○	○	○	—	—	—	○
○			○					Connection integrity	With recovery	—	—	—	○	—	—	○
○			○						Without recovery	—	—	○	○	—	—	○
○			○					Selective field connection integrity		—	—	—	—	—	—	○
○	○		○					Connectionless integrity		—	—	○	○	—	—	○
○	○		○					Selective field connectionless integrity		—	—	—	—	—	—	○
	○		○				○	Nonrepudiation	With proof of origin With proof of delivery	—	—	—	—	—	—	○

○ : Mechanism which is used alone or in combination with another to implement the service.

○ : Provided as an option.
— : Not provided.

*1 : Previously positioned in the presentation layer, but being reexamined.

Figure 5.1.2. Relationship Between Security Services, Mechanisms and Layers

5.1.7 Future development of standardization activities

Although a framework for security architecture is becoming fixed, deliberations on concrete methods for implementing security services have not yet begun. At the ISO, the future development of standardization activities related to security will start with a detailed examination by the SC20/WG1 and WG2 of mechanisms for implementing security services, such as the message authentication and access control mechanisms. Using these mechanisms, SC20/WG3 will examine the concrete implementation methods for security services in each communications function layer. At the present stage, examinations of the physical layer and the transport layer are beginning to be developed. Later, based on the results of examinations by SC20/WG3, the SC in charge of each communications function layer will perform PDU encoding, etc., for each layer. In parallel with these activities, SC21/WG4 is preparing to examine the management elements that can be handled in common in the OSI communication environment, such as the encryption key management and delivery.

5.2 Present Status of Security Technology

There is no clear standard as to how to apply security technology to create a system with a high degree of safety and reliability. The only equivalent to such a standard is the computer system reliability evaluation criteria established by the U.S. Department of Defense in 1983. Because this evaluation criteria is also applicable to applications using information communications networks, the criteria are summarized in a supplement to this Chapter.

Although dated 1983, the criteria were established on the assumption that they would be applied directly to the defense network. Thus it can be seen that the levels that demand very advanced technology are detailed in it.

The levels are defined according to the characteristics summarized below:

Level D: Level satisfying the lowest security requirements.
Level C1: Level up to the data isolation function.
Level C2: Level provided with protection against data access and access control. Immediately higher than Level C1.
Level B1: Level provided with the integrity of security and access control based on it. Immediately higher than Level C2.
Level B2: Level at which structure is used as a security measure. Immediately higher than Level B1.
Level B3: Level in which security procedures or boundaries are defined. Immediately higher than Level B2.
Level A: Highest level provided with inspection techniques for all measures.

When present systems are observed, the majority of operations occur at Level C2 where products made by manufacturers are installed. Even when independent functions are added to them, they go no higher than Level B1.

The target for future progress is very high, but many years may be required until products at Level A become widely used. This means that a great deal of technological development is still necessary.

References

1. Nakao, "Trend of Standardization of Communications Services Used Ciphers," CIS KENKYUU-KAI, 1988.

Supplement

Department of Dtfense

Trusted Computer System Evaluation Criteria

Summary
Background of Materials

An examination of the security safeguards of common resource-type computer systems was started in 1967 at the U.S. Department of Defense. The first report was compiled in 1970, and manuals based on it were completed in 1972 and 1973. Later, as the results of this research were also publicized by the U.S. Air Force, ARPA, and others, a joint research project integrating all of them was started in 1977.

This material is based on the results of this research, but also contains the results of research into technical techniques and evaluation techniques conducted under the leadership of the National Bureau of Standards, as well as an examination of data protection technology commissioned to MITRE. This research and the examinations are compiled and published by the Computer Security Center of the DOD.

(Date of publication stated on the Document: 15 August 1983)

Fundamental Computer Security Requirement

Policy

Requirement 1

"Security Policy"

A clear and defined security policy shall be present in the system.

> With this aim, the objects and actions subject to security shall be defined.

Requirement 2

"Identification Marking"

Objects of security shall be marked with an access control identifier.

Accountability

Requirement 3

"Identification of Action Subject"

Each action subject shall be identifiable.

Requirement 4

"Accountability"

Audit information shall be maintained and protected as required, so that actions related to security violations can be traced and reported to the responsible person.

Assurance

Requirement 5

"Assurance"

To ensure that requirements 1 to 4 are met, computer systems shall be equipped with a hardware or software mechanism that will be evaluated independently for each requirement.

Requirement 6

"Continuous Protection"

A mechanism for improving reliability as described above shall be permanently protected against unnecessary or improper modification.

Chapter 1. Evaluation Criteria

1.0 Division D

Minimal Protection

The only significance of this level is the distinction from the case in which the request for a higher protection level than normal cannot be met.

2.0 Division C

This division has the audit ability and is accompanied with security protection of the object. This division has sublevels that can be selected as required.

2.1 Class C1

Security is provided by isolating the user and the data. Measures for the prevention of accidental data destruction or read-out are also taken here. The minimal requirements for C1 are as follows:

- **Measures**

Access control is provided between the user and object. The access control mechanism uses, for example, file management in which the access rights are categorized as individual, group, common, etc.

- **Responsibility**

User identification and authentication are provided. Examples are the use of passwords.

- **Assurance**

Intervention is data and illegal operations shall be prevented. Also, a periodic inspection shall be performed to check whether the hardware and software functions are operating normally.

- **Assurance related to life cycle**

An inspection will be required to ascertain whether the system is operating as described in its documentation. The inspection is conducted to demonstrate that the user has no means to violate security.

- **Documentation**

—The guide for users shall describe now security is administered between users, in addition to the description of security items.

—The documentation for the system administration personnel shall describe precautions concerning security functions and privileged actions which control the security operations.

—The system developer shall create documentation on the test techniques and results evaluation method.

The documentation shall also show how security functions in the possession of manufacturers are applied. If the security functions are provided as a separate module, a description of the interface is necessary.

2.2 Class C2

This class features a more powerful access protection function. It manages the users individually with respect to the log-in procedure, conducts a broad range of audits on events associated with security, and provides the isolation of resources.

- **Technique**

The access control for security protection shall operate even when the user does not declare it (and naturally in cases when the user specifies it explicitly). When storage areas are allocated initially or reallocated, it shall be ensured that no data are left in these areas.

- **Responsibility**

In addition to Cl, a means that allows the unique identification of individual users shall be provided. Furthermore, the modification of, illegal access to or destruction of the audit trail must be prevented.

The system shall record the following information as an audit trail:

—User identification and authentication functions
—Movement of objects in the user address space
—Deletion of objects
—Actions of computer operators and the system manager
—Action of the security manager

Also, individual records shall contain the following descriptions:

—Date and time of event occurrence
—User
—Type of event
—Event completed or incomplete

In the process of user identification or authentication, it shall be possible to record the point of origin of the request, such as the terminal ID. Also, in the case of the movement or opening of an object, it shall be able to record the name of the object. Furthermore, the system manager shall be able to select and track each of the information items per individual user or user group.

- **Assurance**

In addition to Cl, it shall be possible to isolate the objects individually so that the access control and audit requests can be satisfied.

- **Assurance of life cycle**

In addition to Cl, it shall be possible to inspect and check any data flow violating resource isolation or illegal access against audio data and authentication data.

- **Documentation**

In addition to C1, documents concerning the testing and maintenance of audit files and those concerning the audit recording structure shall be prepared.

3.0 Division B

This division defines the integrity of functions important for security and access control rules that are a mandatory condition.

3.1 Class B1 (Labeled Security Protection)

Class B1 shall include every subject described for C2, and shall label data and provide mandatory items for access management for objects specified by name. Also, any defects notified in tests shall be eliminated completely.

- **Measures**

In addition to C2, labeling is indicated. Sensitivity labels reflecting relative importance are to be attached to each object and memory objects (process, file, segment or device). These labels are used as criteria for determining access control. In case a request concerning nonlabeled data is issued, the system indicates an authorized user to assign a security level to the data. It will be possible to audit and trace all of these actions.

These labels express the security levels of the objects. When labeled data is handed over outside the security system, the internal label shall also be handed over.

When data is transmitted or received through communications, a security level shall be assigned to each line or I/O device. When the data transmission destination is changed, the security level shall be reassigned manually, and this action will be such that it can be audited and traced.

In case several security levels are assigned to an I/O device, control shall be performed so that the security level of the object is transmitted simultaneously, and only to the same medium as the original data recording format.

At the same time, coincidence between the security levels of both the transmitting and receiving parties shall be confirmed by the communications protocol before actual transmission and reception begin. In case one security level is assigned to an I/O device, it is necessary to confirm that the security level of the other party and the security level of the communications circuit coincide.

In case information is output via a communications circuit to a person at a terminal, the security level shall also be assigned to that terminal and display equipment. The system shall be able to mark the security level at the beginning and end of the displayed information (to each page in case of a printer), and to check to ensure that the security level is always maintained correctly. The marking and administration of these security markings shall be such that they can be audited by the system.

- **Access control**

The access control shall be administered for all objects and storage objects of the system, and security levels shall be assigned to all of them. It is natural that two or more security levels will usually be administered. In case there is a hierarchical relationship between security levels:

—A subject can read an object if the subject has an equal or higher level.
—A subject can write information to an object with an equal or lower security level.

- **Responsibility**

In addition to C2, the system is required to have the following functions for the identification and authentication of users:

—Maintenance of recognition data.
—Maintenance of data for determining security levels.

On the other hand, as to auditing, the security level marking shall be audited in order to allow the auditing of communication output data.

- **Assurance**

In addition to C2, process isolation shall be implemented. It is also desirable to provide the documentation to make users understand that security functions are provided and to provide a guide for use in security inspections. Further, it is also necessary to indicate the inspection method for detecting faults in the security function, which should also include the situation of information transfer by communications.

- **Documentation**

The methods used in security administration by the operators and system manager and the operation method for security level changes shall be documented. Also, it is required to provide a guide that enables efficient, consistent security administration by the system in the security management module administration, alarm treatment, and privileged operation administration.

3.2 Class B2 (Security Protection)

The means for carefully classifying and structuring security protection objects and others shall be prepared.

- **Measures**

In addition to B1, the level assignment for direct or indirect resource access from outside the system (or from another system) must be considered. For this, the following administration functions are required.

—The system shall be provided with a function that can detect security level changes immediately as required during conversations between users. Terminal users shall be able to request the system to change the security levels.

—The system shall define the minimum and maximum security levels that can be assigned to the physical equipment. At this time, the physical configuration in which the equipment is used shall also be taken irto consideration.

- **Responsibility**

The system shall support the communication path between users and shall control log-in and authentication by means of it. This path can be activated only from the user side.

- **Assurance**

The system defines its own domain so that its operations are not affected by external intervention or illegal actions. It has a partitioned address space for this objective. Consequently, the system is internally configured by several independent software modules. This allows only the required function models to be administered as occasion demands while the minimum privileged functions are administered permanently.

In addition, it shall be possible to change the operating speeds of the channels connecting external equipment and lines so that the maximum transfer rate can be set individually for each channel.

The inspection shall be capable of inspecting the highest functions. The highest functions describe exceptional events, measures against errors, etc., and a detailed description of them shall make the function check possible.

It is important to place the system configuration management module at the service of the development and maintenance of the system. Its use makes it possible to modify the highest security functions, parameters and documents. The configuration management module shall be assured that it is configured consistently for all documents. Also, it shall allow comparison between previous and new versions.

- **Documentation**

The documentation shall show the mechanism of function inspection and shall include a description of the version generation changes. In addition, the documents shall contain descriptions of the following:

—How illegal use can be prevented.
—How the bypassing of functions can be prevented.
—How proper implementation can be determined.

3.3 Class B3 (Security Domains)

A system equipped with security functions shall not be resistant only to illegal actions, but also compact enough to allow analysis and inspection. Therefore, a design that minimizes complexity is regarded as important.

- **Measures**

An access control list is to be prepared. This list can contain descriptions of individuals, groups, etc.

- **Responsibility**

Steps shall be taken so that authentication paths can be set separately at the time of log-in.

- **Assurance**

International structurization shall be developed and attempts shall be made to provide the hierarchical abstract information and to provide confidentiality of data in this process.

The role of the security manager shall be defined so that the security manager does not have any other functions.

4.0 Division A

This division requires the possession of a formal security inspection technique.

4.1 Class A1 (Verified Design)

The contents are almost identical to B3.

- **Addition to "Assurance"**

It shall also be possible to enter the functions, exceptional events, measures in case of errors, etc., using the formal specifications. However, it shall be made obligatory that, with respect to everything that is utilized in the form of software, hardware or firmware, the master data shall be managed separately.

4.2 Class A1 or above

The classes equal to or above A1 are not specifically described, because they are beyond the current level of technology.

5.3 Future Themes

(1) **The framework for security shall be the subject of further examination**

The implementation of security requires not only measures within the system, but also measures for the network. It is necessary, by enlarging the scope as above, to clarify the framework of each of the security functions and to make efforts leading to their implementation.

(2) **The criteria for security implementation shall be reviewed**

Although the criteria itemized in 1983 by the Department of Defense are a great help, there may be some changes in the actual implementation levels given the fact that now security functions are packaged in ICs. Therefore, it is important to establish reference criteria for the step-by-step improvement of security, taking this into consideration.

(3) **Security implementation policy shall be elaborated more fully**

More detailed examinations shall be conducted for those functions that have already been listed as themes for research but are not regarded as objects of implementation, and their development shall be promoted. On this occasion, it is important to look toward the integration of security administration, focusing not only on the technical elements but taking the necessary relationship with system administration into consideration as well.

This point has many ramifications in terms of supporting the development of key technologies.

Chapter 6. Conclusion

It is not easy to obtain a clear definition of advanced communications. This is because of the frequently different perspectives held by manufacturers, users and carriers. Further, the functional elements of advanced communications sometimes differ individually when an actual application is assumed. But above all, it is because the definition of advanced communications itself varies continuously with rapidly developing information communications technology.

This 3-year research project was started by not thinking of advanced communications as simply the interconnection of networks, but thinking of them more generally as intercommunications made possible by communications functions and communications applications. Also, the objects of the research project were set as items whose technological development is necessary to allow them to exhibit their best effects.

Starting from this objective, in the first year we analyzed the present status of networking among user companies and assessed their needs through a questionnaire. We then used the results of this survey as the foundation of our investigation. At the same time, we also assessed technical systems for advanced communications based on the trends of user needs.

In the second year, we enlarged the scope of our research. We analyzed the technological trends related to the OSI (open system interconnection) system. Here, network interconnections were included in the objects of lower-level communications, and protocol conversion and medium conversion were also added as objects of investigation. We also conducted research into technical and administrative systems for maintaining the communications directory in a network by referring to the results of work on international standardization. They are to be positioned as the technical foundations of advanced communications. Also added as research subjects were policies regarding the utilization of security technology systems that will be required to maintain order in advanced communications. Also added were knowledge processing and AI technology, which are key techniques in dealing with the lack of engineers specializing in the administration of communications. These additions were based on the assumption that their practical use is needed urgently.

The research for FY 1988 was based on the results of the previous years. Since the implementation of the new telecommunications business law, more than 650 carriers have entered the field of telecommunications. In parallel with this, business communications are advancing in terms of both quality and quantity, and the communication utilization policies of a number of companies are changing rapidly as reflected in the emergence of independent communications departments. The research in FY 1988 was conducted based on the understanding of this change in the situation, and efforts were made to clarify the technologies to be developed through the collaboration of administration policy and key technology developers.

Now that we have entered the second year of the practical operation of ISDN, the primary group service and ISDN packet communications service are scheduled to begin. It is also anticipated that, in addition to high-speed digital line services, circuit services that closely match the characteristics of ISDN will be started. These will make it possible to select various communication services. Meanwhile, user networks are configured based not only on economic judgments, but also take into consideration the integration of diverse functions. Virtual private network technology, which is a technology that allows flexible configuration and administration of networks according to applications, is responding to these requirements. In addition, mainly in the United States, the development of intelligent networks (IN) has become a topic with a view to enhancing services in public networks while rendering unique services. ONA (open network architecture) is also attracting attention as a plan in which the user is deeply involved when implementing an IN.

These series of enhancements of service features have become subjects to be examined at the new session term of the CCITT. These examinations will not be like previous examinations, which were started after standards had been established, but will be aimed at providing common concepts for existing events and ideas. The reason why such a phenomenon has appeared is that the commitment to networks is greater than before. As a result, it is necessary to investigate key technologies to embrace permanently changing consciousness patterns and to recognize services as an object of technology. This was the first remark resulting from this research project.

It is not easy to administer a network while managing it, because the objects being managed cover not only communications terminals, communications lines, communications equipment, network component equipment, information processing systems and job applications, but it is also necessary to grasp, in an integrated way, how these objects with different qualities exert an influence on the occurrence of faults. According to another research project, it was shown that deficiencies in network management are growing every year as the networks continue to become more complicated. It has already been noted that the lack of network engineers actually means there is not a sufficient number of management engineers.

In this situation, the concept of network management and administration common to manufacturers, users and carriers has not yet beer sufficiently established. The international standardization of network management is being examined now, but, although the standardization of management information transfer protocols is progressing, the standardization of the scope of information to be managed or the concrete information contents have not yet been clarified. But this is an urgent theme that requires concrete actions as well as an increase in the number of actual examples in order to accelerate these actions. Although it would seem to be an obvious theme, it is an object of very high importance. The second remark determined by this research project is the necessity of being able to recognize developments and to be able to solve actual deficiencies.

It is to easy to correctly implement and administer such an advanced and diversified technological system with a small number of personnel. Using network functions as components and the knowledge of engineers with high-level and advanced abilities as materials, the creation of suitable network administrative structures should be emphasized.

The use of AI technology for this purpose has wide applicability, and benefits can surely be expected. The third remark determined by this research project is to increase the concrete applications of AI technology.

Actual examples of interconnections between company networks are increasing, and this increase shows a tendency toward acceleration as electronic transactions become more widely used. Although there are not many examples of close connections at present because the means of intersystem connections have not been provided sufficiently, the degree of connection is expected to grow following the diffusion of OSI products. The disturbance of American research networks due to hacker attacks in November 1988 is still fresh in our memory. To counteract such threats, the U.S. Department of Defense started examinations early in the seventies and subsequently prepared security criteria. A security system is also provided as a part of the examination of OSI, but this system is being reviewed and work has started to specify the concepts to be referred to for each security item.

A concept for the integration of computer systems and networks is necessary to ensure security. This also necessitates the adoption of common administrative systems for functions such as authentication, isolation and nonrepudiation, as well as security technology such as encryption.

However, present security products do not include this, and there is no example of its independent development. It is necessary not only to point out the increase of losses caused by security violations, but it is also necessary to begin concrete development. The fourth remark determined by this research project is the necessity of evaluating maintenance as a foundation of the information society.

These remarks bring us to the close of this research project. In closing we would like to ask readers to take the rapidly changing situation into consideration when referring to the remarks raised by this research project for the development of key technologies. In this context, we expect that tracing research projects will be executed as the occasion demands. Finally, we express our gratitude to the individuals in the Key Technology center who provided a place for us to conduct our research for 3 years and who provided us with proper guidance. We also express our gratitude to the staff of the Ministry of Posts and Telecommunications and other organizations for their cooperation.

- END -

END OF
FICHE
DATE FILMED
29 March 1990